OPERAATTORITASOISEN REITITYKSEN JA VPLS:N TOTEUTUS SPIDERNETIIN

Marko Vatanen

Opinnäytetyö
Joulukuu 2009

Tietotekniikka
Tekniikka ja Liikenne

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) VATANEN, Marko	Julkaisun laji Opinnäytetyö	Päivämäärä 02.12.2009
	Sivumäärä 124 + 38	Julkaisun kieli Suomi
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty (X)

Työn nimi
OPERAATTORITASOISEN REITITYKSEN JA VPLS:N TOTEUTUS SPIDERNETIIN

Koulutusohjelma
Tietotekniikka

Työn ohjaaja(t)
SILTANEN, JARMO

Toimeksiantaja(t)
Jyväskylän ammattikorkeakoulu Oy
KOHO, JUHA-PEKKA

Tiivistelmä

Jyväskylän ammattikorkeakoulun Teknologia-yksikön SpiderNet-laboratoriota on kehitetty aktiivisesti viimeisen seitsemän vuoden ajan. SpiderNet-laboratoriota käytetään tietoverkkotekniikan opetuksen tukena sekä tutkimus- ja kehitysprojekteissa. SpiderNet tukee useita verkkotekniikoita kuten esimerkiksi: Ethernet, Metro Ethernet, MPLS-VPN, reititysprotokollat.

Opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa operaattoritasoinen reititys ja VPLS SpiderNet-laboratorioon. Reitityksessä keskityttiin lähinnä operaattorien väliseen reittitietojen välittämiseen tarkoitetun BGP:n tutkimiseen eri autonomisten alueiden välillä ja MPLS:n käyttämiseen runkoverkossa.

VPLS on L2-tasolla toimiva operaattoritason VPN-palvelu. VPLS:n avulla operaattorit voivat liittää eri puolella operaattorin runkoverkkoa olevat yritysasiakkaan toimipisteet toisiinsa L2-tasolla. VPLS nopeuttaa liikenteen välittämistä runkoverkoissa verrattuna MPLS-VPN:ään johtuen sen toimimisesta L2-tasolla. VPLS:ssä käytetään joko BGP:llä tai LDP:llä signaloituja virtuaalilinkkejä sekä MPLS-verkkoa kuljettamaan asiakkaan VPN-liikenne.

Työn tarkoituksena oli tutkia VPLS:n eri signalointiprotokollien toimintaa ja Juniper-reitittimien tapaa toteuttaa VPLS-palvelu sekä toteuttaa operaattoritasoinen reititys käyttäen BGP:tä ja MPLS:ää.

Työn tuloksena saatiin todennettua sekä LDP- että BGP-signalointien toimivuus ja vastaavuus standardeihin RFC 4761 ja RC4762.

Avainsanat (asiasanat)
BGP, LDP, Metro Ethernet, MPLS, Reititys, SpiderNet, VPLS

Muut tiedot

Author(s)
VATANEN, Marko

Type of publication
Bachelor´s Thesis

Date
02122009

Pages
124 + 38

Language
Finnish

Confidential

( ) Until

Permission for web publication
(X)

Title
NETWORK OPERATOR LEVEL ROUTING AND VPLS IN SPIDERNET

Degree Programme
Degree Programme Data Network Technology

Tutor(s)
SILTANEN, Jarmo

Assigned by
JAMK University of Applied Sciences
KOHO, Juha-Pekka

Abstract

The data network laboratory SpiderNet in the School of Technology of JAMK University of Applied Sciences has been actively developed for the last seven years. SpiderNet is mainly used in several data network technology courses as well as on various research and development projects. SpiderNet provides a real life environment with multivendor equipment and support for various network protocols, for example: Ethernet, Metro Ethernet, MPLS-VPN and routing protocols.

The aim of the thesis was to design and implement network operator level routing and VPLS in SpiderNet laboratory. The routing was mainly studied to ensure network information propagation between operators and additionally in operator's core network using BGP, LDP and MPLS protocols.

VPLS is a VPN service which operates in Layer-2. With use of VPLS, operators can connect corporate customers sites in Layer-2 level, which speeds the traffic forwarding in core networks compared to MPLS-VPN. VPLS uses either BGP or LDP signaled virtual tunnels and MPLS-backbone to transport customers' VPN traffic.

One of the main goals in the thesis was to study the signal protocols which signal the tunnels between PE devices and to get to know how VPLS works on Juniper routers.

As a result of the thesis signaling of LDP and BGP protocols was proven to be equivalence with the standards RFC 4761 and RFC 4762.

Keywords
BGP, LDP, Metro Ethernet, MPLS, Routing, SpiderNet, VPLS

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

LYHENTEET

AS	Autonomous System
BGP	Border Gateway Protocol
CE	Customer Edge
CLI	Command Line Interface
eBGP	External BGP
FEC	Forwarding Equivalence Class
FIB	Forwarding Information Base
iBGP	Internal BGP
H-VPLS	Hiearchical VPLS
IGP	Interior Gateway Protocol
JUNOS	Juniper Operating System
LAN	Local Area Network
LB	Label Base
LDP	Label Distribution Protocol
LER	Label Edge Router
LFIB	Label Forwarding Information Base
LIB	Label Information Base

LMM	Label Mapping Message
LSI	Label Switching Instance
LSP	Label Switched Path
LSR	Label Switched Router
MAC	Media Access Control
MAN	Metropolitan Area Network
MED	Multiple Exit Discriminator
MPLS	Multiprotocol Label Switching
MTU	Multi-Tenant-Unit tai Maximum-Transfer-Unit
NLRI	Network Layer Reachability Information
OSPF	Open Shortest Path First
PDU	Protocol Data Unit
PE	Provider Edge
PHP	Penultimate Hop Popping
PW	PseudoWire
QinQ	802.1ad standardi
QoS	Quality of Service
RD	Route Distinguisher

RR	Route Reflector
TCP	Transmission Control Protocol
TLV	Type Length Value
TTL	Time To Live
UDP	User Datagram Protocol
VBS	VE Block Size
VE	VPLS Edge
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VSI	Virtual Switch Instance

1 TYÖN LÄHTÖKOHDAT

1.1 Toimeksiantaja

1.1.1 Jyväskylän ammattikorkeakoulu

Työn toimeksiantajana toimi Jyväskylän ammattikorkeakoulu Oy:n (JAMK) tietotekniikan koulutusohjelma. JAMK on monialainen ammattikorkeakoulu Keski-Suomessa, joka tarjoaa useita eri koulutusalueita sisältäen myös mahdollisuuden kouluttautua opettajaksi ammatillisessa opettajakorkeakoulussa.

Jyväskylän ammattikorkeakoulu on vetovoimainen ja kansainvälinen korkeakoulu. JAMK tarjoaa korkeakoulututkintoon johtavaa koulutusta, avoimia ammattikorkeakouluopintoja, täydennyskoulutusta ja ammatillista opettajakoulutusta. JAMKilla on kiinteät suhteet alueen yrityksiin ja yhteisöihin. Työelämä vaikuttaa koulutuksen suuntaamiseen ja opetussuunnitelmien sisältöihin. (Jyväskylän ammattikorkeakoulu 2009.)

1.1.2 Tietotekniikan koulutusohjelma

Tietotekniikan koulutusohjelma JAMK:ssa keskittyy tietoverkko-osaamisen koulutukseen. Koulutusohjelma voidaan jakaa neljään eri ammatilliseen osaamisalueeseen, joista jokainen keskittyy omaan verkkotekniikoiden erityisosaamiseen. CCNP-osaaminen mahdollistaa verkkotekniikoiden ammatilliseen soveltamiseen vaadittavat erityistaidot Cisco Network Academyn, kansainvälisen opintokokonaisuuden kautta. Langattomien tietoliikennejärjestelmien osaaminen sisältää sekä lisensoimattomien että lisensoitujen langattomien tekniikoiden koulutuksen. Verkkopalveluiden laadunhallinnan osaamiseen keskittyvä suuntautuminen sisältää operaattoritasoisien runkoverkkotekniikoiden sekä palvelunlaatuun vaikuttavien tekniikoiden opetuksen. Järjestelmien hallinnan ja tietoturvan osaamiseen keskittyvä suuntautuminen kouluttaa opiskelijan vastaamaan yrityksen verkkojen ja palveluiden tietoturvasta, järjestelmien hallinnasta ja ylläpidosta.

1.2 Työn tavoitteet

Työn lähtökohtana oli toteuttaa Jyväskylän ammattikorkeakoulun tietotekniikka-koulutusohjelman SpiderNet-laboratorioon operaattoritasoinen ympäristö. Työssä käytettiin lähes kaikkia SpiderNetistä löytyvien laitevalmistajien laitteita (Cisco Systems, Extreme Networks, Juniper Networks). Jyväskylän ammattikorkeakoululle hankittiin kevään 2009 aikana viisi kappaletta Juniper Networksin J2320-reititintä, joiden käyttöönotto ja hiearkiaan tutustuminen oli ensimmäinen tehtävä.

Työn pääasiallinen tavoite oli kuitenkin tutkia operaattoritason VPLS-palvelua, joka on pääsiassa suunniteltu yritysten tarvitsemille yhteyksille. Lisäksi tutkittiin operaattorien välistä ja runkoverkon sisäistä reittitietojen vaihtoa BGP-reititysprotokollaa käyttäen.

Tavoitteena oli siis toteuttaa laaja operaattoriverkko SpiderNet-ympäristöön, joka tarjoaisi VPLS-palveluita yritysasiakkaille. SpiderNet-laboratorion laitteet mahdollistavat erillisten runkoverkon ja liityntäverkkojen luomisen, joka on myös tänä päivänä verkko-operaattorien yleisesti käyttämä toteutustapa. Runkoverkkona käytettäisiin Juniper Networksin J2320-reitittimiä ja liityntäverkkoina Extreme Networksin laitteita, joilla toteutettaisiin kaksi erillistä MetroEthernet -rengasta eri puolille runkoverkkoa. Lisäksi toteutettava operaattoriverkko liitettäisiin kahteen erilliseen Cisco Systemsin reitittimeen, jotka yhdessä neljän muun reitittimen kanssa simuloisivat Internetiä tässä toteutuksessa.

Toteutettavassa operaattoriverkossa olisi tarkoitus keskittyä L2-tasoisen VPN-ratkaisun Virtual Private LAN Servicen (VPLS) toimivuuden testaamiseen sekä BGP-protokollan tutkimiseen Juniper Networksin laitteilla. Työn tavoitteena oli myös käyttää BGP:n Route Reflector -ominaisuutta BGP-toteutuksessa.

2 SPIDERNET

2.1 Yleistä

SpiderNet on Jyväskylän ammattikorkeakoulun Teknologiayksikön tietoverkkolaboratorio. SpiderNetiä on kehitetty yli 10 vuoden ajan ja sitä edelleen kehitetään kattamaan uusia tekniikoita, joita käyttävät verkko-operaattorit ja palveluntarjoajat verkoissaan. SpiderNetiä käytetään pääasiassa tietoverkko-koulutusohjelman opintojaksoilla, mutta sitä käytetään myös erilaisissa kehitys- ja tutkimusprojekteissa.

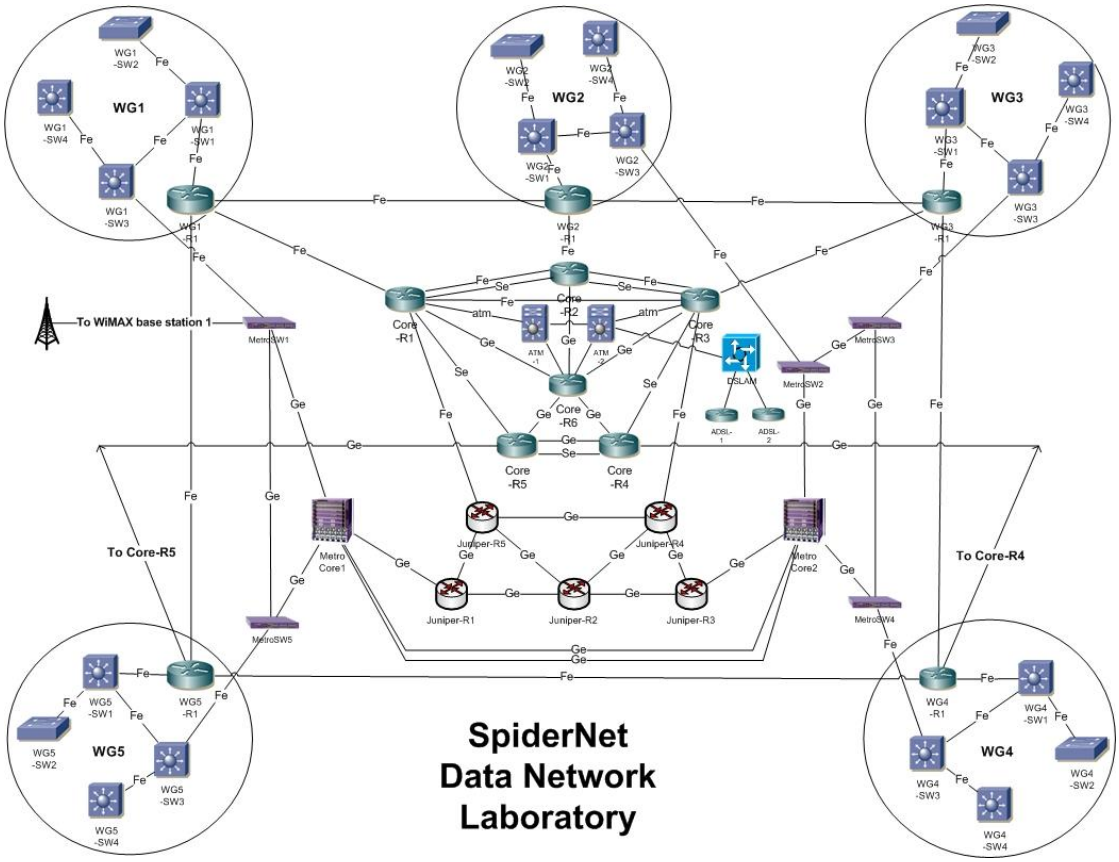
SpiderNet tarjoaa reaalisen ympäristön useiden eri laitevalmistajien laitteilla. Tällä hetkellä laboratoriossa on seuraavien laitevalmistajien tuotteita: Airspan Networks, Cisco Systems, Extreme Networks ja Juniper Networks. SpiderNet koostuu viidestä työryhmästä, Cisco Coresta, Metro Ethernet -alueista ja Juniper Coresta (ks. kuvio 1 tai liite 1).

SpiderNet-ympäristö tukee laajalti eri verkkotekniikoita aina peruslähiverkkotekniikoista kuten VLAN-reitityksestä, IGP-protokollista (EIGRP, IS-IS, OSPF, RIP) ja ADSL:stä, monimutkaisempiin tekniikoihin kuten ATM, BGP, Metro Ethernet (802.1ad, 802.1ah), MPLS-VPN, QoS-mekanismit, VPLS, WiMAX ja niin edelleen.

SpiderNet on täysin eristetty ympäristö ammattikorkeakoulun tuotantoverkosta. Hallintayhteydet SpiderNetin laitteille on toteutettu Cisco Terminal -palvelinta käyttäen. Palvelin kääntää perinteisen lähiverkkoyhteyden konsoliyhteydeksi, mikä mahdollistaa SpiderNetin käytön erillään tuotantoverkosta.

SpiderNetin työasemat ja palvelimet ovat toteutettu virtualisoimalla Linux- ja Windows-työasemia VMware ESX -palvelimella. Jokaisessa työryhmässä on yksi Linux-palvelin ja kaksi Windows-työasemaa. Virtuaalikoneiden avulla SpiderNetin käyttäjien on mahdollista testata toteuttamiaan konfiguraatioita käyttäen eri palveluita ja ohjelmia.

SpiderNet-ympäristössä voidaan testata myös eri laitteiden tukemia jonotus- ja priorisointitekniikoita. Tällä hetkellä SpiderNetissä on käytössä kaksi erilaista liikennegeneraattoria ja –analysaattoria: Interwatch ja JDSU. JDSU-liikennegeneraattorin avulla voidaan verkkoon luoda useita erillisiä liikennevirtoja, joille on mahdollista asettaa useita eri otsikkotietoja aina Ethernet-kehyksestä MPLS- ja VPLS-kehyksiin.



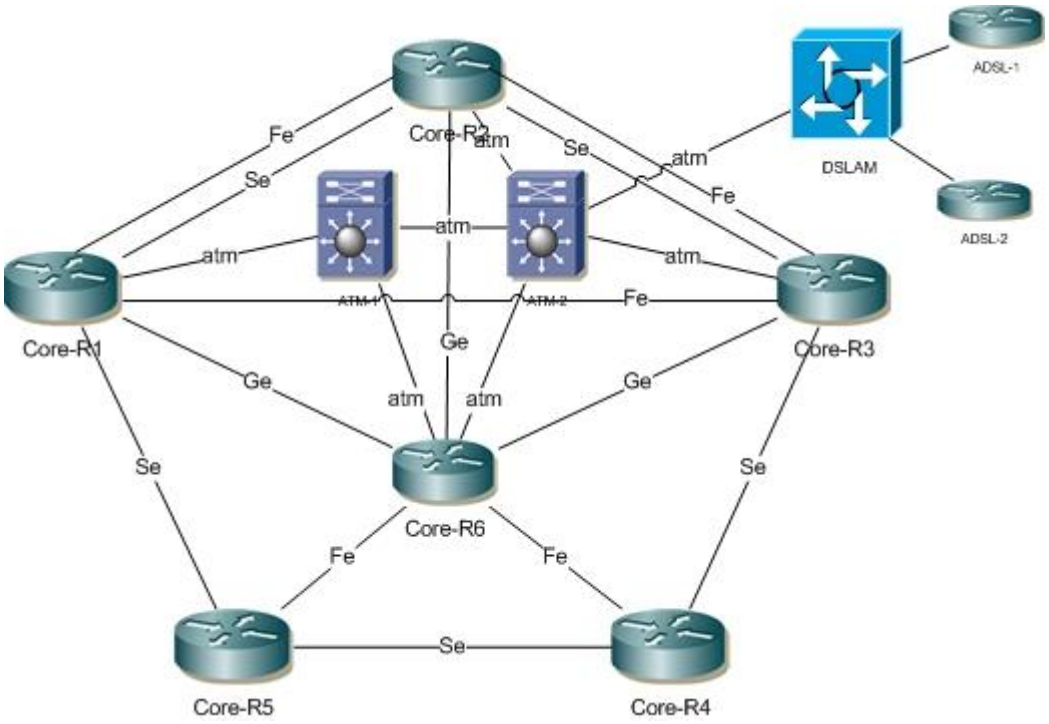
KUVIO 1. SpiderNet-topologia

2.2 Topologia ja laitteisto

SpiderNetiin on mahdollista luoda erilaisia topologiavaihtoehtoja avaamalla tai sulkemalla eri rajapintoja. Tällä hetkellä SpiderNet koostuu neljästä kokonaisuudesta: Cisco Core, Juniper Core, Metro Core ja WorkGroup:t.

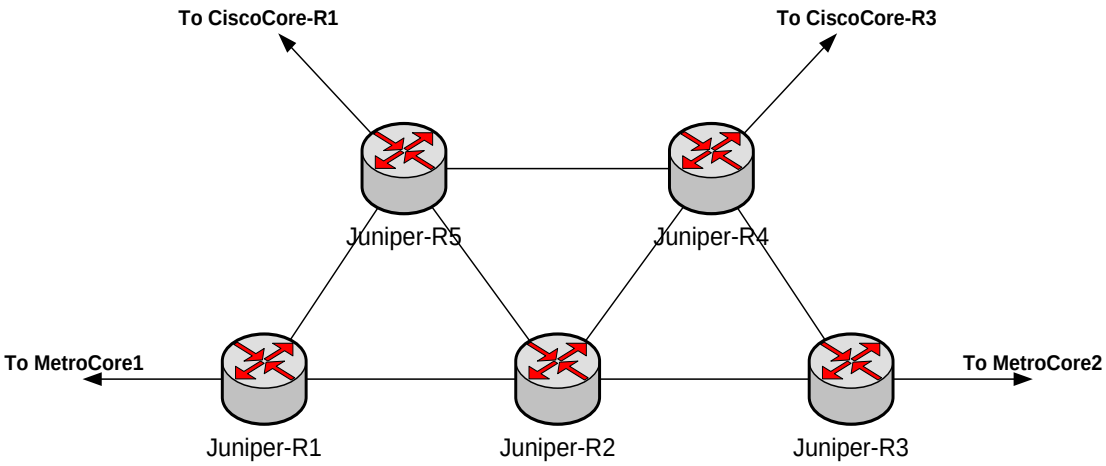
Cisco Core muodostuu kolmesta Cisco Systemsin 3640-reitittimestä sekä kolmesta 7200-reitittimestä kuten kuviosta 2 on nähtävissä. Lisäksi Cisco Coreen kuuluu kaksi ATM-reititintä ja ATM-DSLAM-keskitin sekä neljä hallittavaa ADSL-reititintä. Cisco

Coren viidestä reitittimestä on yhteys vastaavaan WorkGroup:n reitittimeen. Cisco Corea käytetään sekä runkoverkkotekniikoiden että vianhallinnan ja –mittauksen opetuksessa.



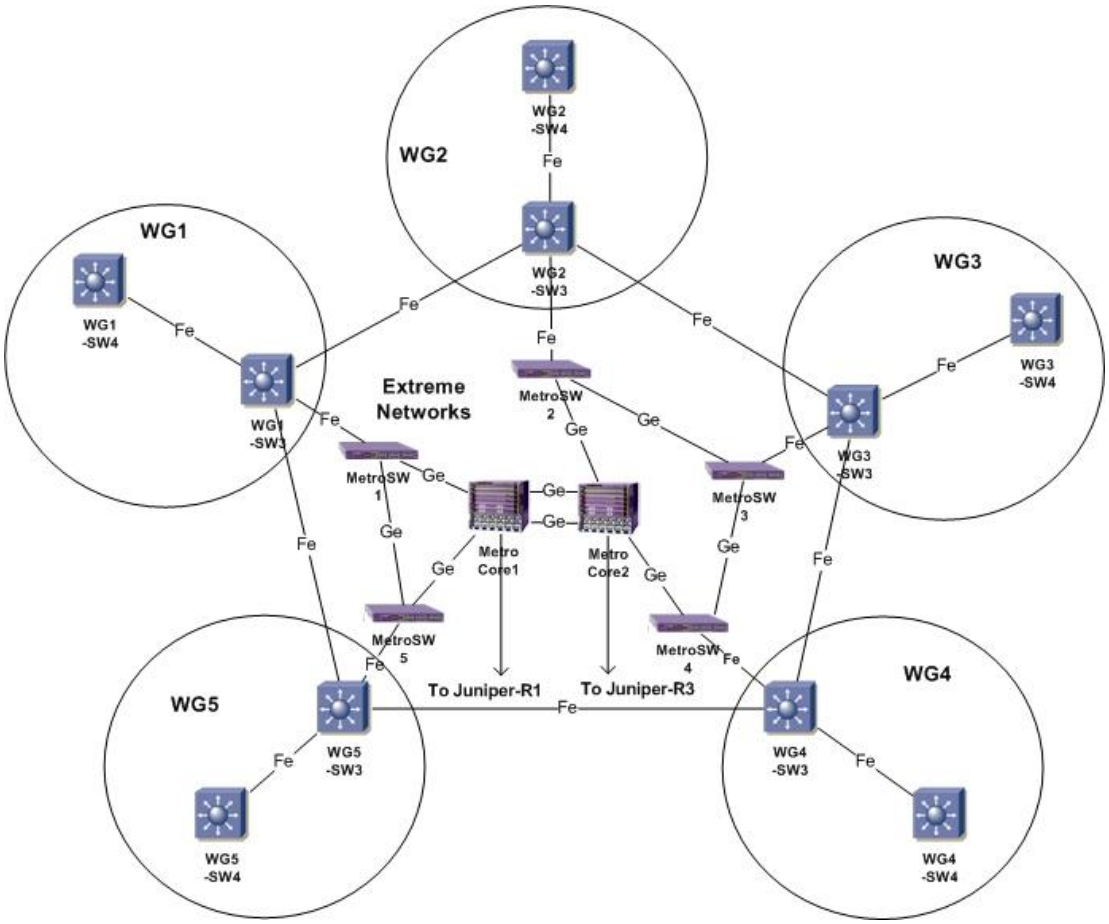
KUVIO 2. Cisco Core -topologia

Juniper Core muodostuu viidestä Juniper Networksin J2320-reitittimestä, jotka ovat mesh-tyyppisesti liitettyinä toisiinsa, ja kaksi J2320-reititintä yhdistää Juniper Coren ja Cisco Coren toisiinsa. Lisäksi kaksi Juniper-reititintä on kytketty Metro Core -kytkimiin (ks. kuvio 3).



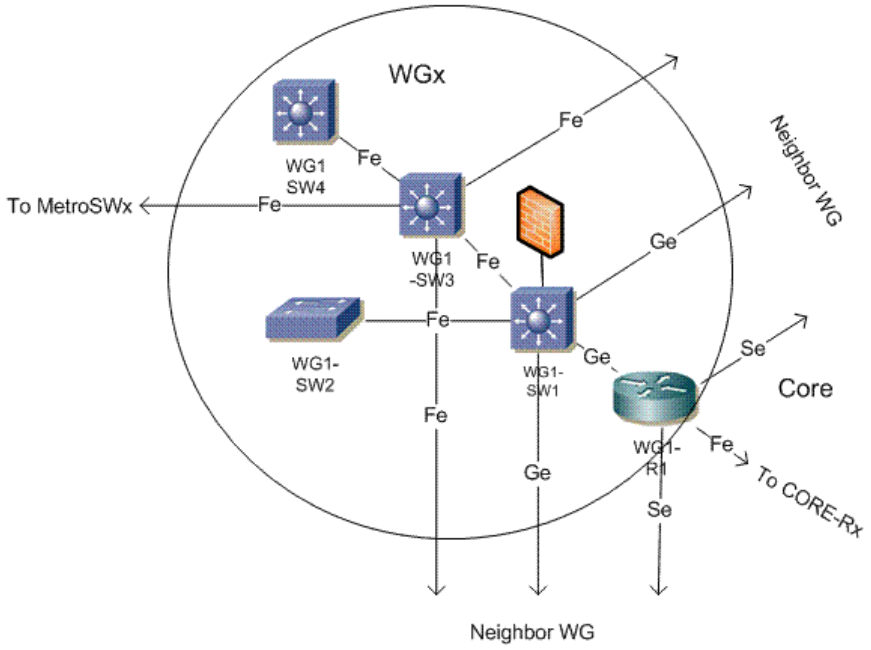
KUVIO 3. Juniper Core -topologia

Metro Core muodostuu kahdesta Extreme Networksin Blackdiamond 12k -kytkimestä sekä viidestä Summit x250 -kytkimestä. Kytkimet muodostavat kaksi erillistä rengasta, mikä mahdollistaa eri Metro Ethernet -alueiden luomisen SpiderNet-ympäristöön (ks. kuvio 4). Blackdiamond-kytkimet toimivat runkokytkiminä ja x250-kytkimet ovat liityntäkytkimiä. Metro Coressa voidaan implementoida seuraavia Metro Ethernet -tekniikoita: EAPS, 802.1ad (QinQ) ja 802.1ah (MAC-in-MAC). Blackdiamond-kytkimet on yhdistetty Juniper Coreen, mikä mahdollistaa mm. VPLS-tekniikan toteuttamisen SpiderNet-ympäristöön.



KUVIO 4. Metro Core -topologia

WorkGroup:t muodostuvat Cisco Systemsin 2821-reitittimestä, Cisco Systemsin 3550 L2/L3-kytkimestä, Cisco Systemsin 2950-kytkimestä sekä kahdesta Extreme Networksin Summit e48-kytkimestä. 2821-reitittimestä on yhteys vastaavaan Cisco Core -reitittimeen (ks. kuvio 5). Toinen Summit e48 -kytkimestä on yhdistetty vastaavaan Metro Core x250 -kytkimeen. Lisäksi jokaisen työryhmän SW1- ja SW3-kytkimet on liitetty naapuri-WorkGroupin vastaavaan SW-kytkimeen. Samoin jokainen WGx-R1-reititin on kytketty naapuri-WorkGroupin R1-reitittimeen serial-yhteydellä.



KUVIO 5. WorkGroup-topologia

3 JUNIPER NETWORKS

3.1 Yritys

Juniper Networks on perustettu helmikuussa 1996. Juniper tarjoaa korkean suorituskyvyn omaavia laitteita, jotka auttavat globaaleilla markkinoilla toimivia palveluntarjoajia, verkko-operaattoreita, suuryrityksiä sekä julkisen sektorin organisaatioita saavuttamaan tuottoa ja kilpailukykyä. Juniper työllistää tällä hetkellä noin 7000 työntekijää 47 eri maassa. Juniperin asiakkaina on 100 suurinta globaalia palveluntarjoajaa, yli 30000 yritystä sekä satoja julkisen sektorin organisaatiota. (Juniper Networks 2009a.)

Juniper Networks on johtava laitevalmistaja skaalautuvissa korkean suorituskyvyn IP-alustoissa. Yritys suunnittelee ja myy ydinverkkoihin tarkoitettuja reitittimiä, jotka hoitavat suurten verkko-operaattorien ja palveluntarjoajien liikenteen reitityksen. Juniper valmistaa lisäksi myös reitittimiin käyttöjärjestelmät (JUNOS) ja tarjoaa koulutusta sekä tukea palveluiden toteutuksissa.

3.2 Laitteet

Juniper Networksin laitteet on jaoteltavissa kahteen pääkategoriaan: reitittimiin ja muihin tuotteisiin. Juniper on pääasiallisesti reititinvalmistaja, mutta se on viime aikoina keskittynyt myös turvallisuusratkaisujen kehittämiseen. Juniper tarjoaa reitittimien lisäksi muuan muassa kytkimiä, palomuureja, VPN-yhdyskäytäviä sekä muita tietoturvalaitteita. (Juniper Networks 2009b.)

3.2.1 Reitittimet

M40-reititin oli ensimmäinen Juniperin valmistama reititin. M40 julkaistiin vuonna 1998 (Juniper Networks 2009a.). Nykyään Juniperin reitittimet voidaan jaotella E-series-, J-series-, M-series- ja T-series-reitittimiin.

Juniper Networks E-series

E-series palvelureitittimet mahdollistavat tehokkaan internetiin liittymisen, IPTV, VoD, VoIP ja interaktiivisten palveluiden tarjoamisen yritys- ja kuluttaja-asiakkaille. E-series-reitittimillä on modulaarinen fyysinen arkkitehtuuri, joka mahdollistaa nopean prosessointitehon. E-seriesin hierarkiset QoS-ominaisuudet takaavat liikenteen laadullisen kuljetuksen, vaikka käytössä olisivat ääni-, video- ja datasovellukset samanaikaisesti yhden fyysisen yhteyden yli.

Juniper Networks J-series

J-series-reitittimet on tarkoitettu lähinnä asiakaslaitteiksi yritysten haarakonttoreihin. J-series reitittimessä on vakiona 4-porttinen GigabitEthernet-kortti ja reititin käyttää modulaarista JUNOS-käyttöjärjestelmää, joka tukee monia kehittyneitä palveluita kuten MPLS, IPv6 sekä tietoturvaominaisuuksia tilallisesta palomuurista IPSec VPN:ään.

Juniper Networks M-series

M-series monipalvelureitittimiä käytetään pääasiallisesti suurissa operaattoritasoisissa verkoissa reunalaitteina, palvelinkeskuksien reunareitittiminä sekä suurien yrityksien pääkonttorien reunalaitteena. M-series reitittimet tukevat useita eri palveluita erilaisista VPN:istä tosiaikaiseen äänen ja videon siirtoon.

Juniper Networks T-series

T-series reitittimet ovat runkoreitittimiä suurten operaattorien runkoverkoissa. Runkoverkoissa tarvitaan skaalautuvuutta välitystasossa, kontrollitasossa sekä palvelutasossa. T-series-reitittimet mahdollistavat suuren suorituskyvyn skaalautuvilla modulaarisilla ratkaisuilla.

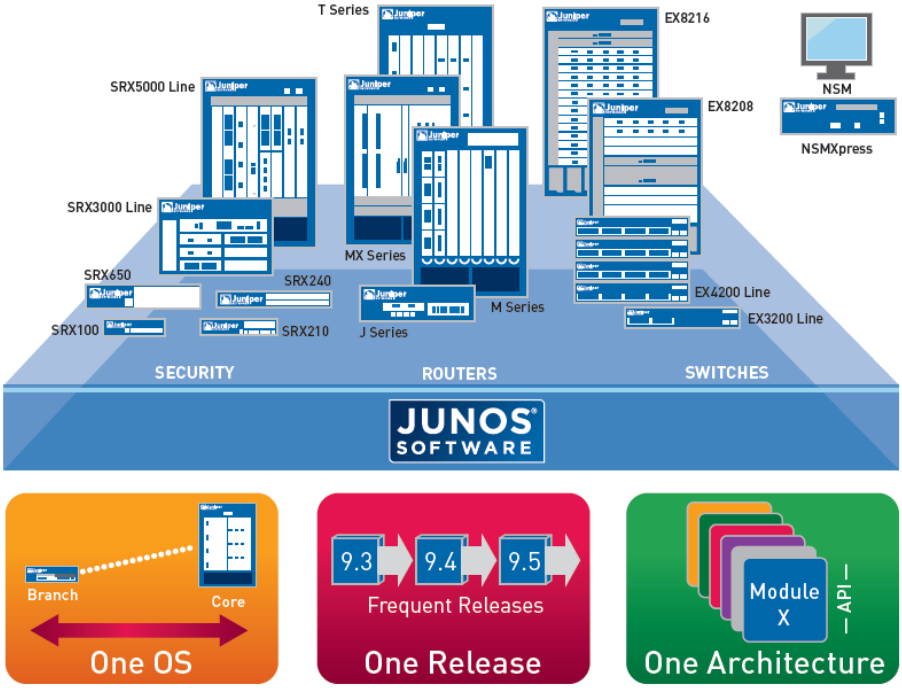
3.2.2 Muut laitteet

Juniper valmistaa reitittimien lisäksi myös muita laitteita, joista merkittävimpiä ovat palomuurit. Juniperin valmistamat EX-series-kytkimet tulivat markkinoille 2008, ja ne käyttävät JUNOS-käyttöjärjestelmää kuten Juniperin valmistamat reitittimet. SRX-series-yhdyskäytävät ovat JUNOSia käyttäviä tehokkaita palomuureja, joissa yhdistyvät tietoturva, reititys ja kytkentä samassa paketissa. SSL VPN -yhdyskäytävät mahdollistavat turvallisten VPN-tunneleiden luomisen eri toimipisteiden välille sekä etäkäyttäjille ilman erillisiä asiakasohjelmia.

3.3 JUNOS

JUNOS eli Juniper Operating System on käyttöjärjestelmä, jota käytetään Juniper Networksin valmistamissa verkkolaitteissa. JUNOS yhdistää reitityksen, kytkennän, tietoturvan ja verkkopalvelut yhteen käyttöjärjestelmään, joka helpottaa korkean suorituskyvyn vaativien verkkojen saatavuuden parantamista sekä uusien palveluiden käyttöönottoa (Juniper Networks 2009c). Juniper käyttää JUNOSia kaikissa sen valmistamissaan verkkolaitteissa riippumatta siitä, onko laite tarkoitettu runkoverkkoon, palomuureiksi vai asiakaslaitteiksi (ks. kuvio 6). Juniper rakentaa JUNOSia vain yhte-

nä “julkaisujunana”, eli Juniper ei kopioi tai käytä uudelleen koodia tehdäkseen erilaisia ominaisuuspaketteja (Juniper Networks 2009c).



KUVIO 6. JUNOS-käyttöjärjestelmä (Juniper Networks 2009c)

JUNOSin ohjelmistoarkkitehtuuri on modulaarinen, mikä mahdollistaa joustavat, vakaat ja innovatiiviset verkkotoiminnot ja alustat. Modulaariset prosessit ajetaan itsenäisesti omassa suojatussa muistissa, joten yksi prosessi ei voi häiritä toisen prosessin toimintaa. Arkkitehtuuri erottaa kontrolli- ja välitystoiminnot toisistaan, mikä mahdollistaa korkean suorituskyvyn ja tehokkaan skaalautuvuuden pienistä laitteista aina erittäin suuriin laitteisiin. (Juniper Networks 2009c.)

JUNOS pohjautuu FreeBSD Unix -käyttöjärjestelmään, mikä mahdollistaa käyttäjien pääsyn Unixin komentokehotteeseen, ja ajaa siellä Unixin komentoja. JUNOS on myös riippumaton käytetystä alustasta, eli JUNOS on sama riippumatta, siitä mitä reititintä käytetään.

JUNOSin ominaisuuksia:

- Reititys
- Kytkentä
- Modulaarisuus
- Tietoturva
- Politiikat ja hallinta
- Standardoidut tekniikat

JUNOSin eniten käytetty käyttöliittymä on perinteinen komentorivi (CLI). CLI jakautuu kahteen tilaan: Operational ja Configuration. Operational-tilaa käytetään laitteen monitorointiin ja vian etsintään, ja sen kautta pääsee myös Configuration-tilaan komennolla *configuration*. Operational-tilassa käytetyimmät komennot löytyvät *show*-komennon alta. Niiden avulla voidaan tarkkailla eri protokollien toiminnallisuutta kuten esimerkiksi tarkistaa reittitaulun tilaa ja niin edelleen. Operational-tilassa suoritetaan myös laitteen käyttöjärjestelmän päivitys. Operational-tilasta on mahdollista siirtyä myös FreeBSD-käyttöjärjestelmän puolelle *shell*-komennolla. FreeBSD:n puolella on käytössä normaalit Unix-käyttöjärjestelmien ominaisuudet. Takaisin CLI:hin pääsee *cli*-komennolla.

Configuration-tila on laitteen konfigurointia varten. Siellä määritetään konfiguraatiomääritykset hierarkian mukaisesti. Hierarkiassa voi liikkua eri tasoille *edit*-komennoilla ja konfiguraatiomääritykset tehdään *set*-komennoilla. Liikkuminen takaisin ylöspäin hierarkiassa voidaan tehdä askel kerrallaan *up*-komennolla tai suoraan ylimmälle tasolle *top*-komennolla. Jokaisella hierarkiatasolla voi katsoa siihen tasoon määritettyjä konfiguraatioita *show*-komennolla. JUNOS ei ota käyttöön asetettuja konfiguraatioita suoraan, vaan käyttäjän on annettava komento *commit*, jotta konfiguraatiot tulevat käyttöön.

4 MULTIPROTOCOL LABEL SWITCHING (MPLS)

4.1 MPLS-tekniikka

MPLS (Multiprotocol Label Switching) on IETF:n (Internet Engineering Task Force) määrittelemä tekniikka, joka lisää tehokkuutta runkoverkkojen reitityksessä, edelleenvälityksessä ja kytkennässä. MPLS mahdollistaa liikenteen välityksen runkoverkkojen läpi ilman tarvetta tehdä reititystä jokaisella hypyllä. MPLS antaa tuen myös muille reitittyville protokollille. Lisäksi MPLS:n avulla on mahdollista toteuttaa erilaisia palveluita kuten esimerksiksi MPLS TE (MPLS Traffic Engineering) ja VPN-tunneleiden muodostaminen MPLS-verkkojen yli.

MPLS-arkkitehtuuri kuvaa mekanismit, joiden avulla suoritetaan leimakytkentää, mikä yhdistää paketin välityksen hyödyntäen L2-tason kytkentää ja L3-tason reititystä (Guichard & Pepelnjak 2001, 11 - 12). MPLS ei tarvitse taustalle toimiakseen muuta kuin toimivan IGP-reititysprotokollan (esim. OSPF tai IS-IS). MPLS-tekniikka liittää paketteihin linkkikohtaisen leiman, jonka perusteella MPLS-reitittimet tekevät liikenteen välityspäätökset. MPLS-reitittimet tekevät leimalle toimintoja (push, pop tai swap) riippuen siitä, mitä paketille tarvitsee tehdä. Reitityspäätöksissä ei siis tarvitse puuttua kuin leiman sisältämään informaatioon ja IP-paketin otsikkotiedot jätetään tutkimatta. IP-otsikkotiedot tutkitaan vain siinä tapauksessa kun paketti poistuu MPLS-verkosta, jolloin perinteinen IP-reititys otetaan käyttöön.

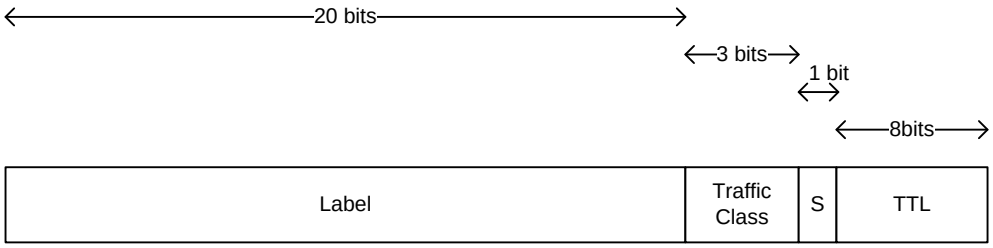
4.1.1 Leima

Leima on lyhyt, kiinteänmittainen paikallisesti merkitsevä tunniste, jota käytetään erittelemään Forwarding Equivalence Class (FEC) eli tietovuo. Leima, joka on asetettu pakettiin, määrittelee FEC:n, johon kyseinen paketti kuuluu. (Callon, Rosen & Viswanathan 2001, 8.).

FEC eli tietovuo on joukko paketteja, jotka välitetään samalla tavalla eteenpäin verkossa. Paketit, jotka kuuluvat samaan FEC:iin, välitetäään samaa polkua pitkin ja ne

saavat samanlaisen kohtelun verkossa. Esimerkiksi samaan IP-otsikon palveluokkaan kuuluvat paketit kuuluvat samaan tietovuohon.

MPLS-leima koostuu neljästä eri kentästä, kuten kuviosta 7 voidaan huomata. Itse leima on 20 bittiä eli se voi saada arvoja väliltä 0 - 1048576. Arvot välillä 0 - 15 ovat varattu tiettyjä toimintoja varten. Traffic Class -bittejä käytetään QoS-priorisointiin. S-bittiä käytetään ilmoittamaan, että kyseessä on pinon alimmainen leima. TTL ilmoittaa elinajan, eli kuinka monta hyppyä paketti voi maksimissaan kulkea. TTL:n avulla estetään MPLS-verkossa ikuisen silmukan syntyminen. (Conta, Farinacci, Fedorkow, Li, Rekhter, Rosen & Tappan 2001, 3 - 5.)



KUVIO 7. MPLS-otsikkotiedot

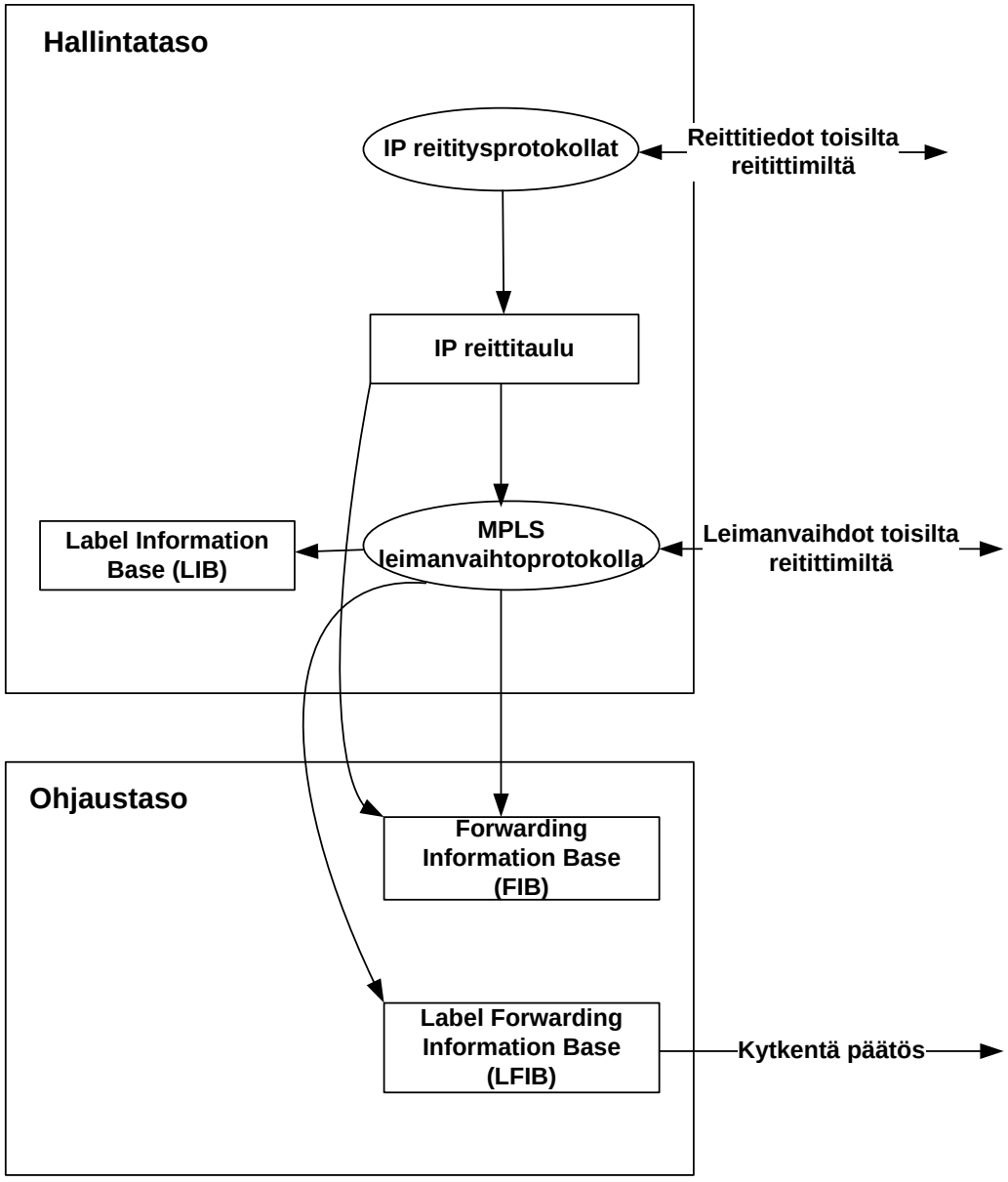
4.1.2 MPLS-verkon toiminta

Paketin saapuessa MPLS-verkon reunalaitteeseen LER:iin (Label Edge Router), reititin tekee perinteisen IP-otsikkotarkastelun ja vertaa kohde IP-osoitetta reititystauluunsa. Tämän jälkeen LER lisää Ethernet-kehyksen ja IP-paketin väliin MPLS-otsikon, johon se asettaa leimanvaihtoprotokollan ennalta määritellyt arvot kyseiselle liikennevuolle. Tämä toiminto luo leimakytkentäisen polun eli LSP:n (Label Switched Path). Paketin kulkiessa läpi MPLS-verkon, jokainen leimakytkentäinen reititin LSR (Label Switched Router) vaihtaa saapuvan leiman lähtevään leimaan. Toimenpidettä voidaan verrata ATM-tekniikkaan, jossa VPI/VCI-arvot vaihdetaan ATM-kytkimien toimesta. (Guichard & Pepelnjak 2001, 17.)

Jokainen LSR pitää yllä reititystaulun lisäksi kahta taulua, jotka ovat relevantteja MPLS:lle. Ensimmäisessä taulussa eli LIB:ssä (Label Information Base) on kaikki leimat, jotka kyseinen LSR on määrittänyt, sekä naapuri LSR:lta saadut leimat. Näitä leimatietoja levitetään käyttäen leimanvaihtoprotokollaa kuten LDP:tä. Toista taulua

eli LFIB:a (Label Forwarding Information Base) käytetään itse pakettien välitykseen ja se sisältää ainoastaan ne leimat, joita käytetään liikenteen välityksessä. (Guichard & Pepelnjak 2001, 18.)

Kuviosta 8 käy ilmi, miten leimakytkentäisten reitittimien hallintataso ja ohjaustaso käsittelevät eri tauluja ja tekevät niiden perusteella kytkentäpäätöksen.



KUVIO 8. MPLS-reitittimen leimakytkentä

4.2 Label Distribution Protocol (LDP)

4.2.1 Yleistä

“MPLS-arkkitehtuuri määrittelee leimanvaihtoprotokollan joukoksi käytänteitä, joiden avulla leimakytkentäinen reititin välittää käyttämiensä leimojen tiedot toisille leimakytkentäisille reitittimille” (Andersson, Minei & Thomas 2007, 5). Label Distribution Protocol (LDP) on leimanvaihtoprotokolla. LDP on yksi käytetyimmistä leimanvaihtoprotokollista MPLS-verkoissa. MPLS-verkoissa leimakytkentäisten reitittimien täytyy sopia eri leimojen tarkoituksista, mitä käytetään pakettien välittämiseen verkossa. LDP määrittelee joukon käytäntöjä ja viestejä, joiden avulla LSR:t välittävät toisilleen käytössä olevien leimojen merkityksen. Leimakytkentäinen reititin käyttää LDP:tä muodostamaan leimakytkentäisiä polkuja läpi MPLS-verkon liittämällä tietyt verkkokerroksen reittitiedot suoraan siirtoyhteyskerroksen kytkettyihin polkuihin. LDP tarvitsee toimiakseen IGP-reititysprotokollan, koska se toimii OSI-mallin kuljetuskerroksella.

4.2.2 LDP viestienvaihto

LDP käyttää neljää eri viestikategoriaa:

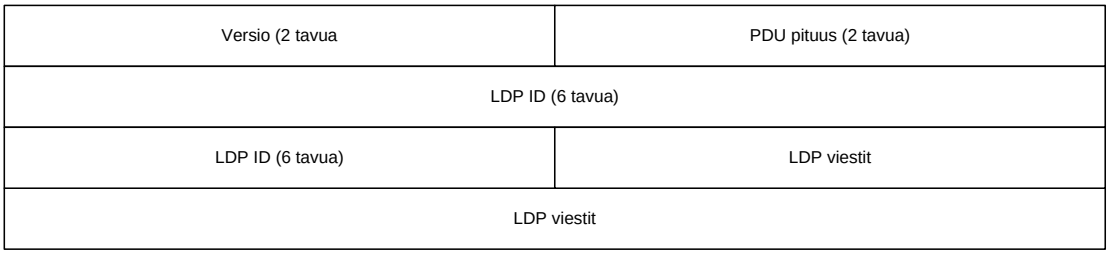
1. Discovery-viestit, joita käytetään ilmoittamaan ja ylläpitämään leimakytkentäisen reitittimien mukanaoloa verkossa.
2. Session-viestit, joita käytetään muodostamaan, ylläpitämään ja päättämään istunnot LDP reitittimien välillä
3. Advertisement-viestit, joita käytetään luomaan, muuttamaan ja poistamaan leimat tietovuoista.
4. Notification-viestit, joita käytetään tuomaan lisäinformaatiota ja havaitsemaan virheellistä informaatiota.

Discovery-viesti on mekanismi, jota käyttämällä leimakytkentäiset reitittimet ilmoittavat läsnäolostaan verkossa lähettämällä Hello-viestejä tasaisin väliajoin. Hello-viesti lähetetään UDP-pakettina LDP:n käyttämään porttiin käyttämällä 224.0.0.2 IP-osoitetta kohdeosoitteena. LSR:n luodessa LDP-istuntoa toisen LSR:n kanssa, se käynnistää LDP-aloituskäytännön TCP-yhteyden ylitse. Onnistuneen istunnon luomi-

sen jälkeen LSR:t voivat alkaa vaihtamaan mainostusviestejä, joissa leimakytkentäiset reitittimet vaihtavat leimakytkentätietojaan. LDP siis tarvitsee luotettavan ja järjestyksenmukaisen viestien siirron. Tämän takia LDP käyttää TCP-yhteyttä session, advertisement- ja notification-viesteille. UDP-protokollaa käytetään ainoastaan Discovery-viesteissä. (Andersson, Minei & Thomas 2007, 6.)

4.2.3 LDP kehysrakenne

LDP:n viestienvaihdot suoritetaan lähettämällä LDP PDU:ja (Protocol Data Unit) LDP-istunnon TCP-yhteyden yli. Jokainen LDP PDU voi sisältää yhden tai useamman LDP-viestin, joiden ei tarvitse olla toisiinsa liittyviä. Kuviossa 9 on kuvattu LDP PDU:n kehysrakenne. Versio-kenttä ilmaisee mitä LDP-versiota käytetään. Nykyinen LDP-versio on yksi (1). PDU pituus kertoo PDU:n kokonaispituuden oktetteina, johon ei sisälly versio ja PDU pituus kenttiä. LDP ID on kuuden oktetin pituinen kenttä, joka yksiselitteisesti identifioi paketin lähettävän leimakytkentäisen reitittimen leimatilan. (Andersson, Minei & Thomas 2007, 6.)



KUVIO 9. LDP-kehys

LDP-viestit ovat Type-Length-Value-kehysrakenteella (TLV) merkattuja viestejä. Periaatteessa kaiken LDP:n PDU:ssa näkyvä tulee olla kehystettynä TLV-merkkausta käyttäen. Kuviosta 10 on nähtävissä TLV-kehys. TLV-kehys koostuu:

- U-bitistä, joka on Unknown TLV-bitti
- F-bitistä, joka on Forward Unknown TLV-bitti
- Type-kentästä (14 bittiä), jossa on LDP-viestin tyyppi
- Length-kentästä (16 bittiä), jossa on LDP-viestin pituus oktetteina
- Value-kentästä (muuttuvan mittainen, jossa on LDP-viestin arvot

KUVIO 10. TLV-kehys

5 METRO ETHERNET

5.1 Yleistä

Ethernet-pohjaista Metropolitan Area Network:a (MAN) kutsutaan yleisesti Metro Ethernet -verkoksi MEN (Metro Ethernet Network). Metro Ethernet -tekniikan nimi on muodostunut Metropolitan Area Network (MAN) määritelmästä, sekä siinä käytettävästä Ethernet-tekniikasta. Metro Ethernet -tekniikka hyödyntää perinteistä Ethernet-tekniikka, jonka vahvuuksia ovat helppokäyttöisyys, kustannustehokkuus ja joustavuus. (Metro Ethernet Forum 2009.)

Metro Ethernet -tekniikka on yleistynyt pitkälti sen takia, että suurin osa suurten yritysten verkoista on Ethernet-pohjaisia. Tästä syystä on järkevintä, että Ethernet alkaa ja päättyy Ethernet-porttiin yrityksissä. Metro Ethernet on luonnollinen vaihtoehto liittyä palveluntarjoajan verkkoon, kun lähiverkossa on muutenkin käytössä Ethernet-tekniikka. Metro Ethernet -tekniikka mahdollistaa myös suuremmat liityntänopeudet. Nykypäivänä Metro Ethernetin kautta tarjottavat liityntänopeudet ovat 1Mbps:n ja 10Gbps:n välillä. Tulevaisuudessa on mahdollista entisestään kasvattaa liityntänopeuksia, kun Ethernet-tekniikan uudet nopeusmääritykset saadaan standardoitua. (Metro Ethernet Forum 2009a.)

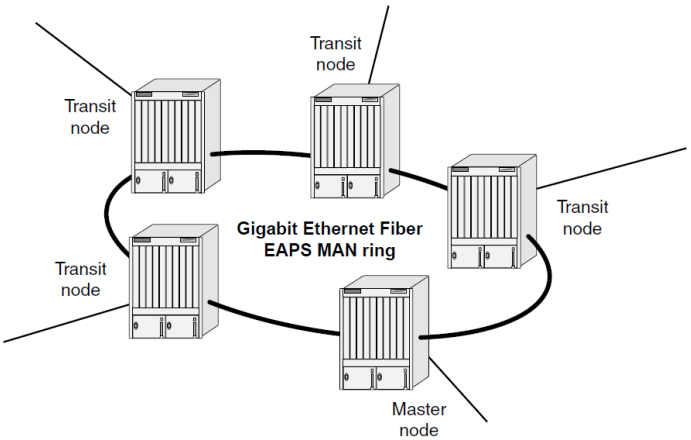
Metro Ethernet -verkoissa käytettävästä Ethernet-tekniikasta johtuen sillä on myös Ethernet-tekniikan perusongelmat ja rajoitukset. Näitä ovat mm. törmäysalueet, tuplakehysten lähetysongelmat, MAC-osoitetaulujen hallitsematon kasvu sekä verkon liikenteen hallinointi.

5.2 Ethernet Automatic Protection Switching (EAPS)

Ethernet Automatic Protection Switching (EAPS) on Extreme Networksin kehittämä silmukanestoprotokolla rengastopologioihin. EAPS on OSI-mallin toisella kerroksella toimiva protokolla, jolla varmistetaan ettei esim. MAN-verkoissa synny silmukoita. Metro Ethernet -verkkojen rengastopologioihin EAPS tarjoaa oivan ratkaisun, koska EAPS:ssa on nopea viasta toipumisaika (noin 50ms), se skaalautuu hyvin suuriin verkkoihin, EAPS tarjoaa luotettavaa loogista ja fyysistä segmentointia sekä sisältää helposti ennustettavan ja johdonmukaisen viasta palautumistavan. Koska EAPS:ia käytetään rengastopologioissa (ks. kuvio 11), silmukoiden estäminen tapahtuu katkaisemalla liikennöinti isäntäsolmun secondary-portissa. (Extreme Networks 2009, 811).

EAPS-rengastopologiaan kuuluvat seuraavat osat (Extreme Networks 2009, 812):

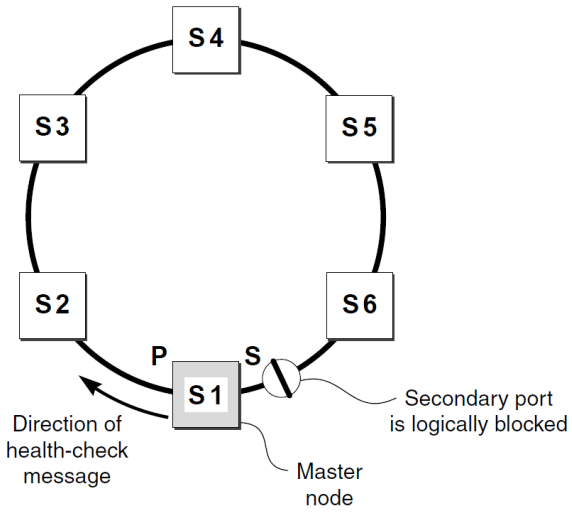
- Yksi isäntäsolmu (Master Node)
- Yksi tai useampi välityssolmu (Transit Node)
- Yksi hallinta VLAN-verkko (Control VLAN)
- Yksi tai useampi asiakas virtuaaliverkko (Protected VLAN)
- Fyysiset kaapelit



KUVIO 11. EAPS-rengastopologia (Extreme Networks 2009, 813)

Kuviossa 12 on kuvattu yksikertaisen EAPS-renkaan toimintaperiaate. Isäntä-solmun porteista toinen on määritetty ensisijaiseksi portiksi ja toinen portti on toissijainen

portti. Asiakasliikenne kuljetetaan omissa VLAN:eissa eli Protected VLAN:eissa, jotka sidotaan EAPS-renkaan portteihin leimattuina. Hallintaliikenne kulkee yhdessä määritellyssä VLAN:ssa, jota kutsutaan Control VLAN:ksi. Normaali toiminnassa isäntäsolmu sulkee loogisesti toissijaisen portin kaikelta muulta liikenteeltä paitsi hallintaliikenteeltä. Tämä toimintaperiaate estää silmukan syntymisen renkaaseen vastaavasti kuin Spanning Tree Protocol sulkee loogisesti linkkejä. Isäntäsolmu lähettää Health-Check-viestejä ensisijaisesta portista toissijaiseen porttiin, kun rengas on muodostettu. Tällä toiminnolla isäntäsolmu valvoo renkaan eheyttä. Mikäli isäntäsolmu ei vastaanota Health-Check-viestejä Fail-timer ajan kuluessa toissijaisesta portista, se muuttaa renkaan Failed-tilaan ja avaa loogisesti suljetun toissijaisen portin. Tämän jälkeen isäntäsolmu tyhjentää oman kytkentätaulunsa ja lähettää välityssolmuille Flush FDB -viestin, jolla kehotetaan muita kytkimiä tyhjentämään kytkentätaulunsa ja opettelemaan MAC-osoitteet uudestaan. (Extreme Networks 2009, 812 - 814.)

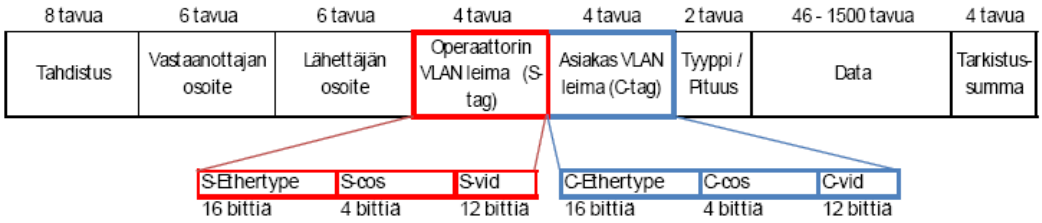


KUVIO 12. EAPS-renkaan toiminta (Extreme Networks 2009, 814)

5.3 IEEE 802.1ad

IEEE 802.1ad, jota myös QinQ:ksi kutsutaan, on standardi, joka on jatkokehitystä 802.1q teknisille rajoituksille. Perinteinen IEEE 802.1q -standardi mahdollistaa vain 0 - 4096 (VLAN ID -kenttä = 12bittiä) eri VLAN:ia. IEEE 802.1ad on ratkaisu Metro Ethernet -palveluntarjoajille, minkä avulla on mahdollista kuljettaa VLAN-liikennettä useilta eri asiakkailta yhteisen verkon läpi. (Extreme Networks 2009.)

IEEE 802.1ad -standardin ideana on lisätä normaaliin 802.1q leimattuun Ethernet-kehykseen toinen 802.1q leima (ks. kuvio 13). 802.1ad-kehyksessä on kaksi neljän tavun VLAN-leimaa. S-tag on ns. operaattorin VLAN-leima, jonka avulla erotellaan eri asiakkaiden liikenteet omiin VLAN:hin. Tämä mahdollistaa sen, että asiakkaiden käyttämät leimat (C-tag) kulkevat koskemattomina Metro Ethernet -verkon läpi.



KUVIO 13. 802.1ad-kehys

802.1ad leima asetaan kehykseen sen saavuttua ensimmäiseen Metro Ethernet-kytkimeen. Tämän jälkeen kehys liikennöi Metro Ethernet-verkon läpi pelkästään ensimmäisen leimatiedon perusteella. Kehyksen saavuttua viimeiseen Metro Ethernet-kytkimeen, siitä poistetaan ensimmäinen leima, minkä jälkeen liikennöinti tapahtuu asiakkaan verkossa asiakas VLAN leiman perusteella.

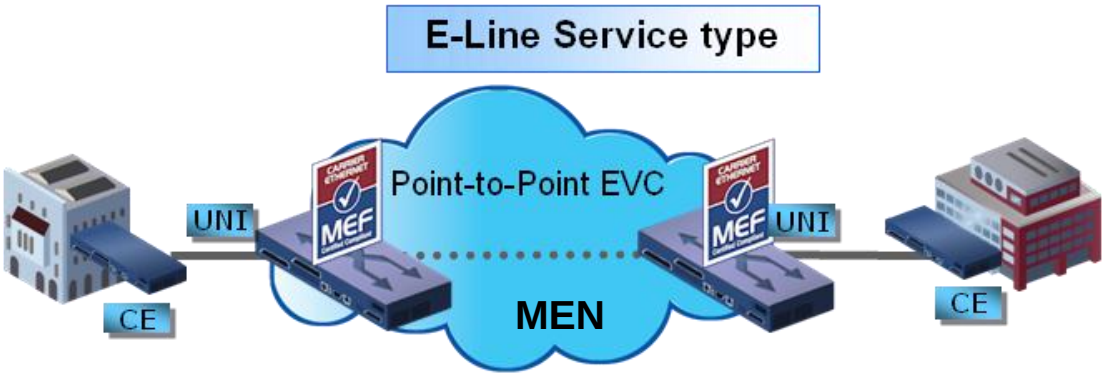
Koska 802.1ad on suunniteltu paikallisiin Metro Ethernet-liityntäverkkoihin, tulee sen rajat vastaan (vain reilut 4000 operaattoritunnelia) laajoissa verkoissa. Tätä varten Metro Ethernet Forum on kehitellyt IEEE 802.1ah standardin, joka laajentaa tunneleiden määrän runkoverkoissa noin 16.7 miljoonaan. Koska tässä työssä ei käytetty 802.1ah standardia, ei sen toimintaa käsitellä tarkemmin.

5.4 Metro Ethernet palvelut

5.4.1 E-Line

Ethernet Line Service (E-Line) on pisteestä pisteeseen palvelu, jossa kaksi eri käyttäjärajapintaa voidaan yhdistää toisiinsa virtuaaliyhteyksillä (Ethernet Virtual Connection, EVC) Metro Ethernet -verkoissa (ks. kuvio 14). E-line palvelulla yhdistetään kaksi käyttäjärajapintaa kahdensuuntaisella yhteydellä, jos tulee tilanne, jossa tarvitsee lisätä

uusi käyttäjärajapinta, on lisättävä myös uusi virtuaaliyhteys kaikkiin verkon käyttäjärajapintoihin. (Metro Ethernet Forum 2009b.)



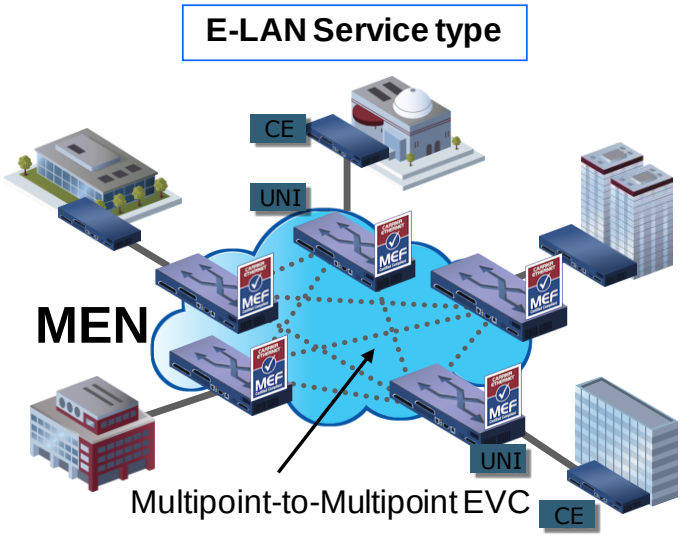
KUVIO 14. E-line-palvelu (Metro Ethernet Forum 2009b)

E-line palvelulla on mahdollista toteuttaa seuraavat palvelut (Metro Ethernet Forum 2009b.):

- Ethernet Private Line: Yksityinen Ethernet-yhteys kahden eri käyttäjärajapinnan välille
- Virtual Private Line: Virtuaalinen kahden eri käyttäjärajapinnan välinen yhteys
- Ethernet Internet Access: Ethernet-yhteys Internetiin

5.4.2 E-LAN

Ethernet LAN (E-LAN) palvelu on multipoint-to-multipoint yhteys, joka yhdistää useampia eri käyttäjärajapintoja virtuaalisilla yhteyksillä (ks. kuvio 15) (Metro Ethernet Forum 2009b).



KUVIO 15. E-LAN-palvelu (Metro Ethernet Forum 2009b)

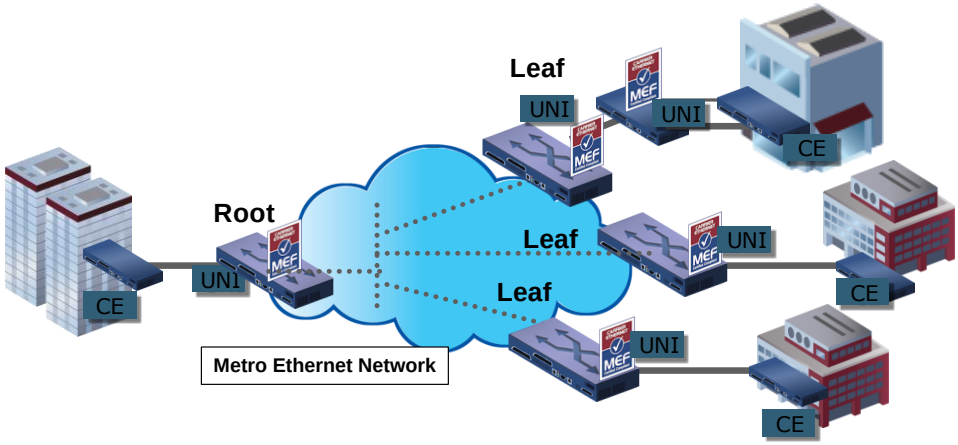
E-LAN palvelua voidaan käyttää toteuttamaan useita erilaisia palveluita. Yksinkertaisimmillaan E-LAN palvelu on Best Effort palvelu ilman suorituskyky takuita. Kehittyneemmissä muodoissa E-LAN palvelu voi määritellä yhteyksille viiverajoja, viiveenvaihtelurajoja sekä suorituskykytakeita. E-LAN palvelu näkyy käyttäjälle normaalina lähiverkkona, vaikka oikeasti palvelu toteutetaan Metro Ethernet-verkon läpi. E-LAN palvelulla voidaan helposti liittää suurikin määrä verkkoja yhteen, koska uuden käyttäjärajapinnan tuominen verkkoon vaatii ainoastaan sen liittämisen oikeaan EVC:hen. (Metro Ethernet Forum 2009b.)

E-LAN palvelulla saadaa luotua seuraavat palvelut (Metro Ethernet Forum 2009b.):

- Multipoint L2 VPN: Useaan pisteen L2 VPN-yhteys
- Transparent LAN Service: Läpinäkyvä LAN-palvelu, esim. VPLS
- IPTV-mahdollisuus sekä multicast-verkko

5.4.3 E-Tree

Ethernet Tree (E-Tree) palvelulla tarkoitetaan point-to-multipoint yhteyttä, jossa yksi käyttäjärajapinta voidaan yhdistää moniin eri käyttäjärajapintoihin virtuaaliyhteyksillä (ks. kuvio 16) (Metro Ethernet Forum 2009b).



KUVIO 16. E-Tree-palvelu (Metro Ethernet Forum 2009b)

E-Tree palvelussa liikenne voidaan erotella toisistaan. Yhdestä haarasta (Leaf) ei voi liikennöidä toiseen haaraan, mutta sallittaan yhteys juureen (Root). Palvelu on tarkoitettu moni-isäntä- ja franchising-sovelluksiin, joissa käyttäjien liikenne tulee pitää läpinäkyvinä muille käyttäjille. (Metro Ethernet Forum 2009b.)

6 VIRTUAL PRIVATE LAN SERVICE (VPLS)

6.1 Yleistä

Virtual Private LAN Service (VPLS), joka tunnetaan myös nimillä Transparent LAN Service ja E-LAN Service, on virtuaalinen lähiverkkopalvelu. VPLS-palvelun avulla on mahdollista toteuttaa VPN-palveluita L2-tasolla. VPLS yhdistää useita erillillään olevia lähiverkkoja operaattorin pakettikytkentäisen verkon läpi siten, että asiakkaalle lähiverkot näkyvät ja käyttäytyvät yhtenä lähiverkkona. (Kompella & Rekhter 2007, 3.)

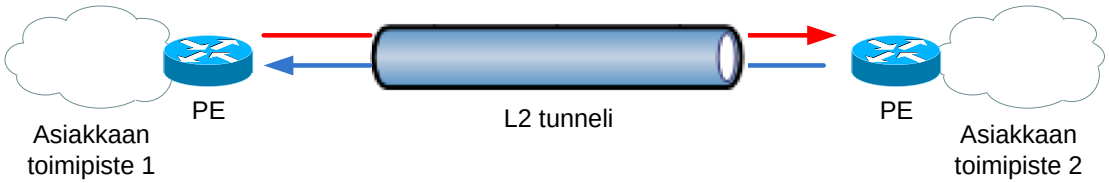
VPLS yhdistää Ethernetin kustannustehokkuuden IP/MPLS-verkkojen liikenteensiirtoon, liikenteenhallintaan, skaalautuvuuteen ja luotettavuuteen tarjoten L2-tason Ethernet-pohjaisia monipistevirtuaaliverkkoja. VPLS tarjoaa Ethernet-palveluja, jotka voivat levittäytyä yhden tai useamman MAN-verkon alueelle ja näin muodostaa yhden loogisen lähiverkon. Virtuaaliverkot ovat palveluita, joita palveluntarjoajat tarjoavat yritysasiakkailleen. Virtuaaliverkkojen avulla palveluntarjoajat voivat yhdistää useita asiakkaiden toimipisteitä turvallisesti yleisesti käytössä olevan verkon läpi. (Juniper Networks 2009d, 4.)

VPLS nopeuttaa liikenteen käsittelyä, koska paketin määränpään selvittämiseksi ei tarvitse osoitetarkastelua tehdä kuin L2-kerrokselle asti. Osoitetarkastelu on verkkolaitteiden menetelmä selvittää paketin edelleenlähetysosoite. Osoitetarkastelussa käydään läpi paketin hyötykuorman lisäksi liitetyt osoitetiedot, joiden perusteella tehdään edelleenlähetys. Mitä alemmalla OSI-mallin kerroksella tämä osoitetarkastelu tehdään sitä nopeampi on pakettien välitys verkossa.

6.2 VPLS:n ominaisuuksia

6.2.1 Virtuaalilinkki

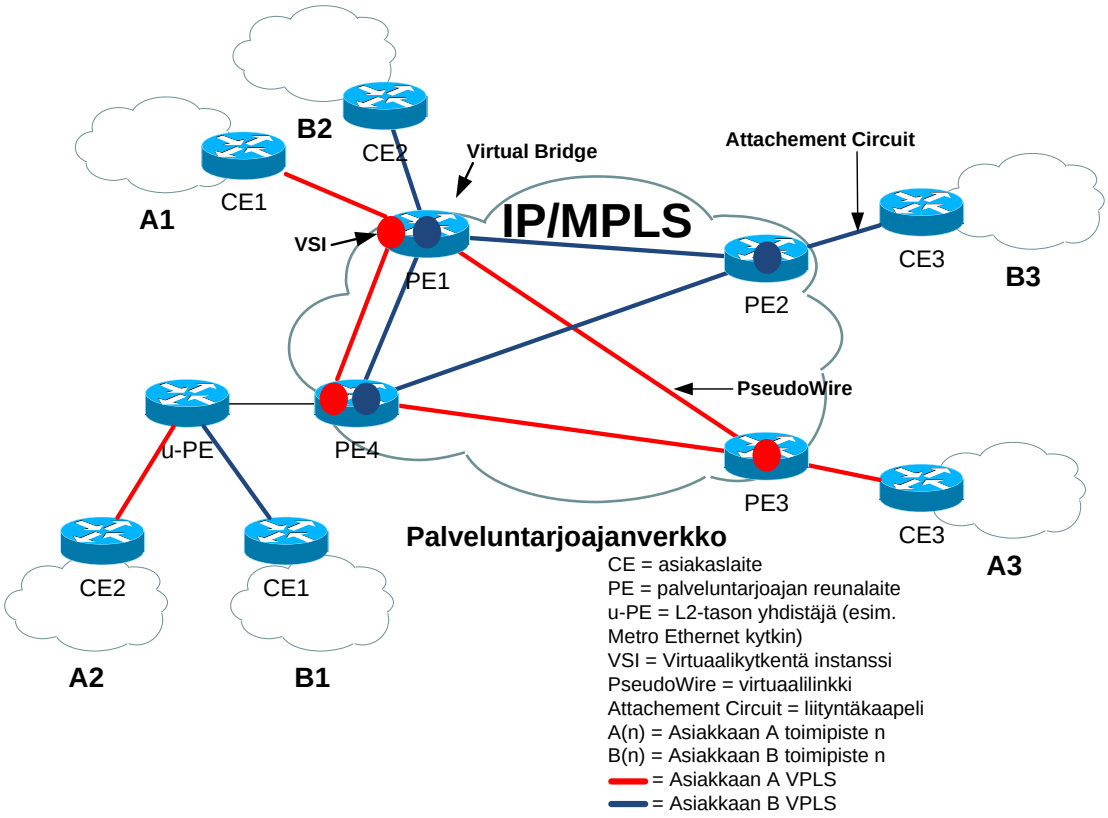
Virtuaalilinkki eli PseudoWire mahdollistaa Ethernet/802.3 PDU:den kuljettamisen MPLS-verkon läpi. Virtuaalilinkkiemulaatio reunalta reunalle (Pseudo Wire Emulation Edge-to-Edge, PWE3) on mekanismi, jonka avulla kuljetetaan Ethernet-liikennettä esimerkiksi pakettikytkentäisen verkon (Packet Switched Network, PSN) läpi. Virtuaalilinkkien tärkeitä ominaisuuksia ovat PDU:den kapselointi, kuljettaminen polun tai tunnelin läpi, ajoituksen ja järjestyksen hallinta sekä muut vaadittavat operaatiot palvelun emuloimiseen. Kuten kuviosta 17 on nähtävissä, virtuaalilinkit ovat pisteestä pisteeseen yhteyksiä, jotka ovat vain yhden hypyn mittaisia ja vastakkaisia toisilleen eli ne ovat kahden laitteen välisiä LSP:tä. LSP on merkattu virtuaalilinkkileimalla (PW-label), jota kutsutaan myös virtuaaliyhteysleimaksi (VC-label). Virtuaalilinkkien leimanvaihto tapahtuu joko BGP:n tai LDP avulla palveluntarjoajan PE-laitteiden välillä. Samalla laitteet vaihtavat VPLS-tunnistetietoja, jotka mahdollistavat virtuaalilinkkien liittämisen tiettyyn VPLS-instanssiin.



KUVIO 17. Virtuaalilinkki

6.2.2 VPLS:n referenssimalli

Kuviossa 18 on esitetty VPLS:n referenssimalli. Asiakkaan CE-laite on liitettynä palveluntarjoajan PE-laitteseen, joka sitoo CE-laitteen sille määritettyyn VPLS-instanssiin (Virtual Switch Instance, VSI). Asiakaspään laite voi olla joko kytkin tai reititin, mikäli oletetaan, että palveluntarjoajan rajapinta on Ethernet-liityntä. Asiakaslaitteen ja palveluntarjoajan reunalaitteen välistä linkkiä kutsutaan liityntäkaapeliksi (Attachement Circuit). PE-laite hallinnoi VPLS-yhteyksien aloituksia ja lopetuksia sekä vastaa vaadittavien tunneleiden muodostuksesta muiden palveluntarjoajan verkkolaitteiden kanssa. PE-laitteen täytyy hallita MAC-osoitteet, pakettien replikointi ja uudelleenlähetykset sekä yhdistää opitut osoitteet tiettyihin virtuaalilinkkeihin (PseudoWire). Jokainen PE-laitteen VSI luo virtuaalilinkin toiseen PE-laitteeseen, jossa on samaan VPLS-instanssiin kuuluva asiakaslaite. Jokaista VPLS-instanssia varten on PE-laitteen luotava virtuaalilinkki toiseen PE-laitteeseen. Käytettäessä MPLS-verkkoa eri PE-laitteiden välillä, verkossa täytyy olla leimakytkentäisiä polkuja (LSP) yhtä paljon kuin on VPLS:ien välisiä linkkejä (Juniper Networks 2009d). Tästä aiheutuu täysinkytketty topologia LSP-polkuja PE-laitteiden välille. IP/MPLS-verkko yhdistää palveluntarjoajan verkkolaitteet toisiinsa. Verkko ei itsessään ota kantaa VPN-toimintoihin, vaan ainoastaan välittää liikennettä MPLS-leimakytkennän avulla.



KUVIO 18. VPLS-referenssimalli

6.2.3 VPLS:n toiminta

VPLS-verkko on periaatteessa yksi iso kytkin. Se muodostaa virtuaalilinkkejä PE-laitteiden välille ja läpinäkyvästi kuljettaa L2-tason kehyksiä muodostettuja virtuaalilinkkejä pitkin. Palveluntarjoajan PE-laitteet oppivat lähde MAC-osoitteet ja luovat MAC-kytkentä tietueen välittäessään kehyksiä. PE-laitteet saavat näin luotua kytkennät MAC-osoitteiden ja liityntäkaapelien tai virtuaalilinkkien välille. MPLS-verkon P-laitteet ainoastaan välittävät paketteja perustuen MPLS-leimoihin ilman, että ne ovat edes tietoisia sisällä kulkevasta L2-tason asiakaskehyksistä.

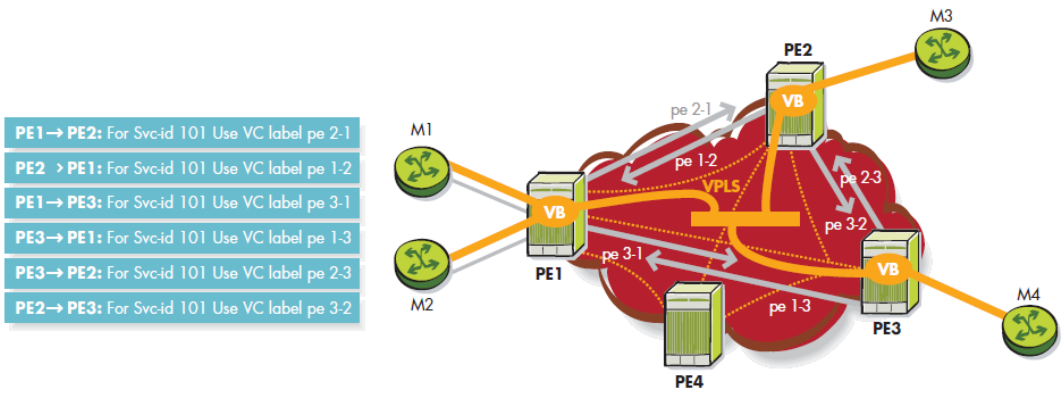
PE-laite pystyy vastaanottamaan Ethernet-kehyksiä asiakkaan toimipisteestä ja kytkemään kehyksiä perustuen niiden MAC-osoitteeseen oikeaan leimakytkentäiseen polkuun, kun MPLS-verkossa on leimakytkentäiset polut olemassa jokaisen VPLS-instanssin välillä. Tämä on mahdollista, koska VPLS mahdollistaa PE-reitittimen toimia ns. Learning Bridge:nä eli jokaista VPLS-instanssia kohti PE-laitteessa on MAC-osoitetaulu. MAC-osoitetaulua täydennetään opituilla MAC-osoitteilla, kun Ethernet-

kehykset saapuvat tiettyyn fyysiseen tai loogiseen rajapintaan. PE-laitteen toiminta on täysin vastaavaa kuin perinteisen Ethernet-kytkimen. (Juniper Networks 2009d, 4.)

Ethernet-kehyksen saapuessa asiakkaan toimipisteeseen kytkettyyn rajapintaan, ensimmäisenä PE-laite tarkastaa kohde MAC-osoitteen ja vertaa sitä MAC-osoitetauluun. Kehys lähetetään muuttumattomana leimakytkentäiseen polkuun, joka välittää kehyksen oikeaan PE-laitteeseen, johon on kytketty toinen asiakkaan toimipiste. Mikäli MAC-osoitetta ei löydy osoitetaulusta, kehys monistetaan ja lähetään kaikkiin liityntäkaapeleihin tai virtuaalilinkeihin, jotka kuuluvat samaan VPLS-instanssiin poislukien se rajapinta, josta kyseinen kehys saapui. Kyseinen toiminto vastaa monien protokollien käyttämää Split Horizon -silmukanestotekniikkaa, jossa PE-laite tulvittaa kaikki kehykset (tuntematon Unicast-, Broadcast- ja Multicast-kehys), joiden kohde-MAC-osoitetta ei ole MAC-osoitetaulussa, muihin rajapintoihin paitsi siihen, josta kyseinen kehys vastaanotettiin. Split Horizon -tekniikka estää PE-laitetta lähettämästä tuntemattoman MAC-osoitteen omaavaa pakettia muihin virtuaalilinkkeihin, mikäli se vastaanottaa sellaisen virtuaalilinkistä. (Kompella & Lasserre 2007, 6 - 7.)

Esimerkki VPLS:n toiminnasta

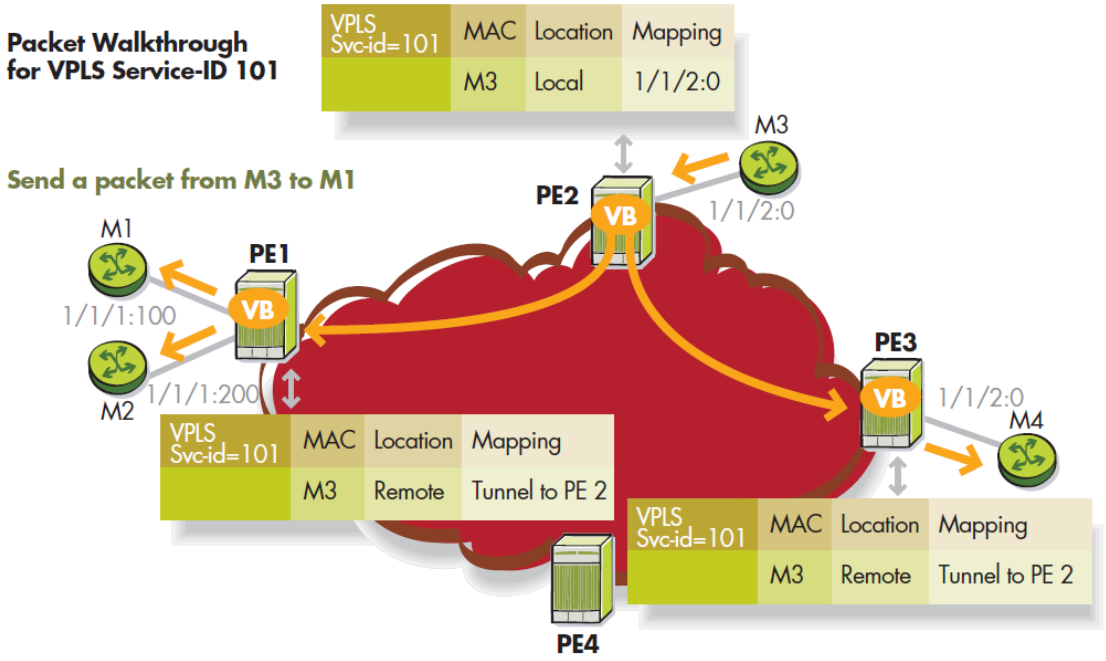
Oletetaan, että palveluntarjoajan MPLS-verkossa on täysinkytkettyjä MPLS-tunneleita neljän PE-laitteen välillä. VPLS-instanssi tarvitsee olla luotuna PE1-, PE2- ja PE3-laitteiden välille ja se on määritelty esimerkiksi ID:llä 101. M1-M4 ovat asiakkaan eri toimipisteitä ja niiden liityntäkaapelit ovat kytkettyinä vastaaviin PE-laitteisiin. Kuvissa 19 on nähtävissä virtuaalilinkkien käyttämät Virtual Circuit -leimat. Virtual Circuit -leimat ovat VPLS-signalointiprotokollan muodostamia virtuaalipolkujen leimoja, joita käytetään tunnistamaan eri VPLS-instanssien välisiä virtuaalilinkkejä. Kun VPLS-instanssi on muodostettu, PE-laitteet aloittavat leimojen vaihtoprosessin. Tämän jälkeen ensimmäiset paketit voidaan lähettää eri toimipisteiden välillä ja MAC-osoitteiden oppiminen alkaa. (De Clercq, Khandekar & Witters 2009.)



KUVIO 19. Virtuaalilinkkien signalointi (De Clercq, Khandekar & Witters 2009.)

Kuviossa 20 on kuvattu tilanne, jossa toimipisteestä M3 lähetetään paketti, joka on kohdistettu toimipisteeseen M1 (De Clercq, Khandekar & Witters 2009.):

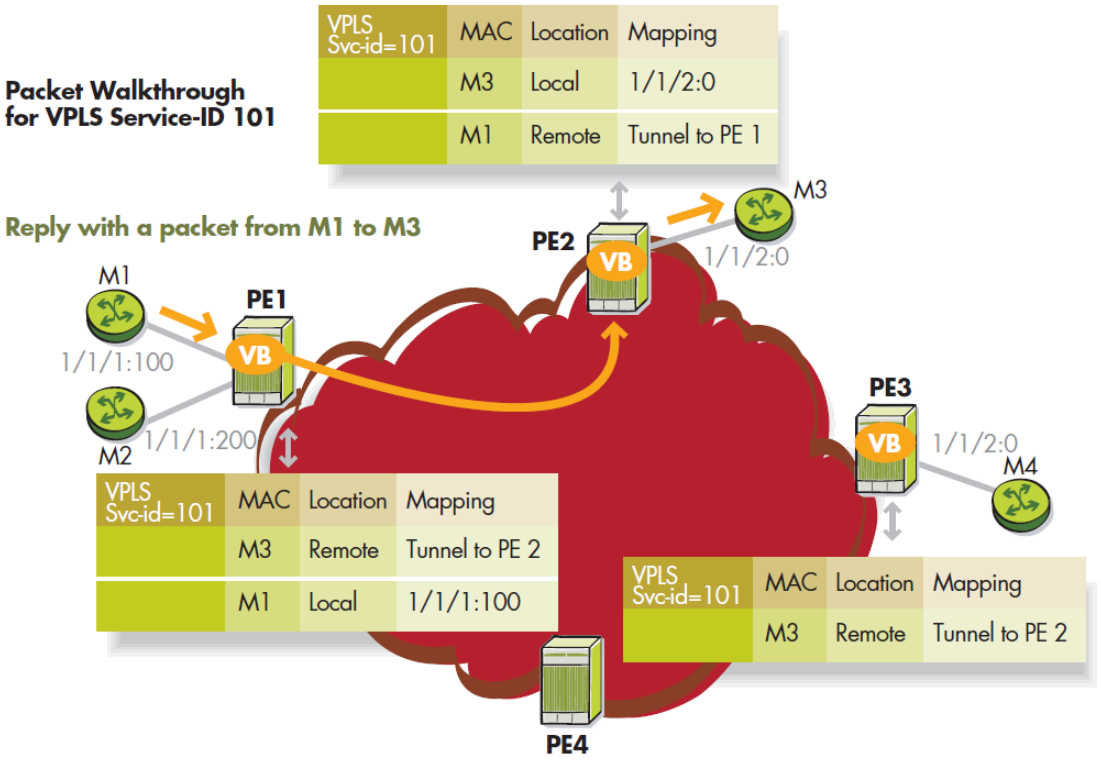
1. PE2-laite vastaanottaa paketin ja oppii paketin lähde MAC-osoitteen sekä liittää sen paikalliseen porttiin 1/1/2:0.
2. PE2-laite ei tässä vaiheessa tiedä kohde MAC-osoitetta M1-laitteeseen, joten se tulvittaa paketin PE1-laitteelle käyttäen VC-leimaa *pe2-1* ja PE3-laitteelle VC-leimalla *pe2-3*.
3. PE1-laite oppii VC-leimasta *pe2-1*, että M3 on PE2-laitteeseen kytketty.
4. PE3-laite oppii vastaavasti VC-leimasta *pe2-3*, että M3 on PE2-laitteeseen kytketty.
5. PE1-laite poistaa VC-leiman, mutta koska kohde MAC-osoitetta ei ole ko. VPLS-instanssin MAC-taulussa se tulvittaa paketin kaikkiin paikallisiin portteihin, jotka kuuluvat ko. VPLS-instanssiin.
6. M1 vastaanottaa paketin



KUVIO 20. VPLS:n MAC-osoitteiden oppiminen (De Clercq, Khandekar & Witters 2009.)

Kuviossa 21 M1 vastaa uudella paketilla M3:lle vastaanotettuaan paketin (De Clercq, Khandekar & Witters 2009.):

1. PE1-laite vastaanottaa paketin ja oppii samalla, että M1 on paikallisessa portissa 1/1/1:100.
2. PE1-laite tietää jo, että M3 voidaan tarvoittaa PE2-laitteen kautta, joten se lähettää paketin ainoastaan virtuaalilinkkiä pitkin PE2-laitteelle käyttäen VC-leimaa *pe1-2*.
3. PE2-laite vastaanottaa paketin, joka on kohdistettu M3:lle. PE2-laite tietää edellisen paketin perusteella, että M3 on tavoitettavissa paikallisen portin 1/1/2:0 kautta.
4. M3 vastaanottaa paketin.



KUVIO 21. VPLS:n paketinvälitys (De Clercq, Khandekar & Witters 2009.)

6.2.4 Auto Discovery

Jokaiselle VPLS-instanssille on määritettävä globaalisti uniikki tunniste. Usein tästä käytetään myös nimitystä VPN-ID. Eri signalointi menetelmissä käytetään eri tunnisteita, mutta nykyisistä VPLS-signaloinnissa käytössä olevista protokollista ainoastaan BGP tukee Auto Discovery -ominaisuutta.

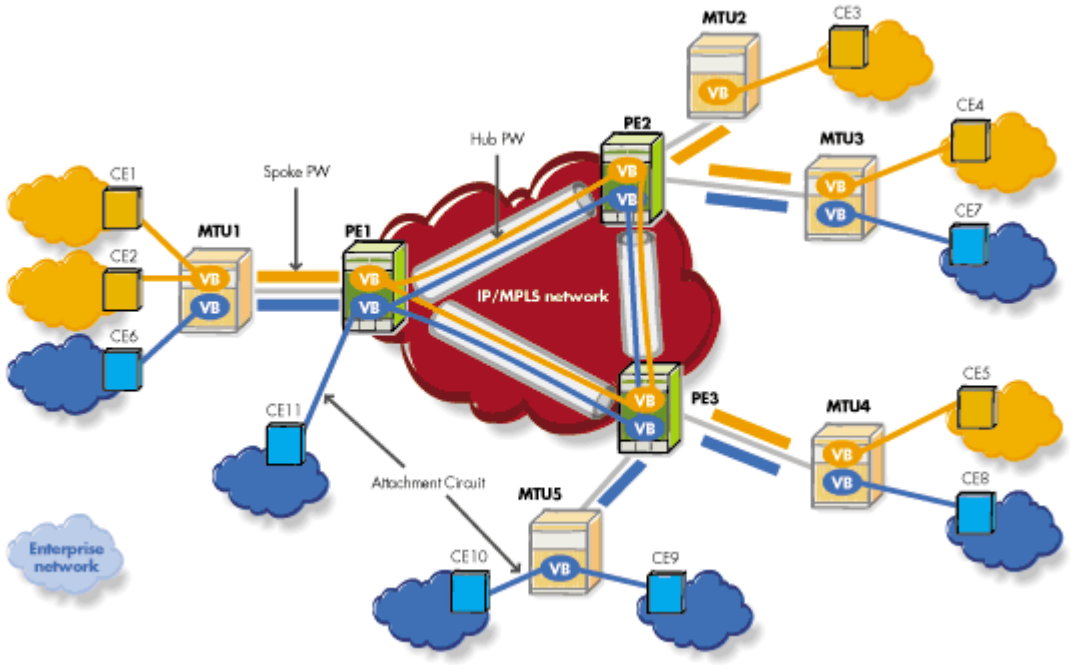
Kun uusi PE-laite lisätään VPLS-alueeseen (esimerkiksi PE-laitteen alueelle tulee asiakkaan uusi toimipiste, joka halutaan liittää VPLS-alueeseen), PE-laite mainostaa, että se kuuluu myös ko. VPLS-alueeseen käyttäen BGP-viestejä. Tämän jälkeen tieto kulkee kaikille VPLS-alueeseen kuuluville PE-laitteille, jotka tulevat tietoisiksi uudesta PE-laitteesta ja niillä on kaikki tarvittava tieto, jota tarvitaan muodostamaan leimakytkentäinen polku uuteen PE-laitteeseen automaattisesti. (Juniper Networks 2009d, 5.)

LDP:n tapauksessa RFC 4762 ei määrittele Auto Discovery -ominaisuutta, mistä aiheutuu palveluntarjoajalle enemmän ylläpidollista toimintaa, koska konfiguroidessa

uutta PE-laitetta VPLS-alueeseen on ylläpitäjän tiedettävä kaikki PE-laitteet, jotka ovat mukana kyseisessä VPLS-alueessa. LDP:tä käytettäessä voidaan toki käyttää muita protokollia/palveluita Auto Discovery -ominaisuuden saavuttamiseksi, kuten esimerkiksi RADIUS-palvelinta.

6.2.5 H-VPLS

Hierarkinen VPLS eli H-VPLS perustuu VPLS-ratkaisuihin ja laajentaa sitä useilla skaalautuvuus ja toiminnallisuus parannuksilla. Hierarkista VPLS ratkaisua käytetään varsinkin laajoissa toteutuksissa, joissa on lukuisia PE-laitteita ja/tai Multi Tenant -kytkimiä (MTU). Palveluntarjoajat sijoittavat MTU-kytkimet rakennuksiin, joissa on useiden eri yritysten toimipisteitä, joista jokainen voi kuulua eri VPLS-alueeseen. MTU-kytkin voi olla mikä tahansa Ethernet-kytkin, joka tukee kaikkia L2-kerroksen toimintoja, esimerkiksi Metro Ethernet -kytkin. PE-laitteiden suuri määrä voi johtaa skaalautuvuusongelmiin lähinnä johtuen suuresta määrästä virtuaalilinkkejä, pakettien monistuksesta sekä MAC-osoitteiden suuresta määrästä. H-VPLS tukeutuu hierarkiseen malliin, jossa ei tarvita täysinkytkettyä ratkaisua leimakytkentäisille poluille. Hierarkia saavutetaan yhdistämällä VPLS-ydinverkon virtuaalilinkit liityntä virtuaalilinkkeihin muodostaen näin kaksitasoisen hierarkisen VPLS-mallin (ks. kuvio 22). (De Clercq, Khandekar & Witters 2009.)



KUVIO 22. H-VPLS-referenssimalli (De Clercq, Khandekar & Witters 2009.)

H-VPLS-referenssimalli jakautuu keskus (Hub) PE-laitteisiin ja haara (Spoke) PE-laitteisiin. Keskuslaitteiden väliset virtuaalilinkit ovat keskusvirtuaalilinkkejä (Hub PW), joiden sisällä kaikkien VPLS-alueiden liikenne välitetään. Haara PE-laitteisiin on yleensä kytkettynä MTU-kytkin, jonka kautta eri VPLS-alueisiin kuuluvat toimipisteet yhdistetään. MTU-kytkimen ja PE-laitteen välisiä virtuaalilinkkejä kutsutaan haaravirtuaalilinkeiksi (Spoke PW). H-VPLS vähentää virtuaalilinkkien määrää isoissa verkoissa, koska lisättäessä uutta VPLS-alueeseen liittyvää toimipistettä ei tarvitse kuin konfiguroida MTU-kytkimen ja PE-laitteen välinen virtuaalilinkki.

BGP-signalointia käytettäessä H-VPLS:n toteuttamiseen voidaan käyttää reittiheijastimia eli Route Reflector:eja. Ideana on suunnitella pieni joukko reittiheijastimia, jotka ovat keskenään täysinkytkettyjä. BGP-osapuolen ja yhden tai useamman reittiheijastimen välille muodostetaan BGP-yhteys. Tällä tavalla ei ole välttämätöntä luoda suoria täysinkytkettyjä BGP-yhteyksiä jokaisen VPLS-instanssin PE-laitteen välille. Jos reittiheijastimia on suuri määrä voidaan tätä ideaa käyttää myös rekursiivisesti eli luodaan useampia hiearkiatasoja. (Kompella & Rekther 2007, 17.)

6.3 VPLS käyttäen BGP-signalointia

VPLS-verkon muodostamiseen voidaan käyttää kahta eri signalointiprotokollaa. BGP-signalointi on määritelty RFC4761:ssä, jossa on myös määritelty Auto Discovery -ominaisuus.

BGP-signalointia käytetään virtuaalilinkkien muodostamiseen sekä purkamiseen PE-laitteiden välille eli käytännössä signalointi vaihtaa leimatietoja PE-laitteiden välillä. Signalointia käytetään myös virtuaalilinkkien ominaisuuksien välittämiseen, jotka PE-laite luo tietylle VPLS:lle. VPLS:ssä BGP:n käyttäminen mahdollistaa sekä Auto Discovery:n että signaloinnin. Kun BGP-signalointia käytetään VPLS-verkossa, tarvitsee PE-laitteiden välille luoda iBGP-yhteys. iBGP tarvitsee toimiakseen täysin kytketyn verkon BGP-istunnoin, mikä mahdollistaa VPN-ID:den käyttämisen osallistuvien PE-laitteiden välillä. Täysin kytketty verkko mahdollistaa täydellisen listan kaikista PE-laitteista kyseisellä VPN-alueella. (Kompella & Rekther 2007, 1 - 8.)

BGP Update -viestien käyttäminen leimatietojen välittämiseen jokaiselle PE-laitteelle vaatisi lähettävältä laitteelta n-kappaletta viestejä n-kappaleelle PE-laitteita. BGP-signaloinnissa PE-laite lähettää ainoastaan yhden yhteisen Update-viestin, joka sisältää leimatiedot kaikille PE-laitteille. Yksi yhteinen Update-viesti vähentää kontrollitason kuormitusta viestejä lähettävissä reitittimissä sekä BGP-reittiheijastin reitittimissä. Tämän mahdollistamiseksi BGP-signaloinnissa käytetään leimaryhmiä (label block), jonka määrittelee LB (label base) ja VBS (VE block size). Leimaryhmä on jatkuva sarja leimoja (LB, LB+1, ..., LB+VBS-1). Tiettyyn VPLS-alueeseen kuuluvat PE-laitteille määritetään konfiguraatioissa uniikki VE ID (VPLS Edge Identifier). PE-laitteen X lähettäessä VPLS-päivityksen, lähetetään sama leimaryhmätieto kaikille PE-laitteille. Jokainen vastaanottava PE-laite päättelee leiman, joka on tarkoitettu PE-laitteelle X, lisäämällä oman VE ID:n leimaryhmään. Tällä tavalla jokainen päivitysviestin vastaanottava PE-laite saa uniikin leiman PE-laite X:lle kyseiseen VPLS:een. (Kompella & Rekther 2007, 8.)

VPLS:n BGP NLRI -paketti

VPLS:n BGP-signaloinnissa käytetään BGP NLRI -paketteja (Network Layer Reachability Information) VPLS-jäsenyyden ja VPLS-leimojen vaihtamiseen. VPLS:n BGP NLRI:ssä on seuraavat informaatiokentät: VE ID, VE Block Offset, VE Block Size ja Label Base. Kuviossa 23 on esitetty VPLS:n BGP NLRI -informaatiokehys. (Kompella & Rekther 2007, 9.)

Length (16bittiä)
Route Distinguisher (64 bittiä)
VE ID (16 bittiä)
VE Block Offset (16 bittiä)
VE Block Size (16 bittiä)
Label Base (24 bittiä)

KUVIO 23. VPLS:n BGP NLRI -informaatiokehys

PE-laite, joka kuuluu ainakin yhteen VPLS-alueeseen, tarvitsee vähintään yhden VE ID:n. Mikäli PE-laite on kytkettynä useaan u-PE-laitteeseen, sillä on erilliset VE ID:t jokaiselle u-PE-laitteelle. VE ID:t konfiguroi verkon hallintohenkilöstö ja ne ovat paikallisia tiettyyn VPLS:een. Annettu VE ID tulee kuulua ainoastaan yhteen PE-laitteeseen, ellei CE-laite ole ns. multi-homed eli se on kytkettynä kahteen tai useampaan PE-laitteeseen. Leimaryhmä (Label Block) on joukko leimoja, joita käytetään tavoittamaan annettu VE ID. (Kompella & Rekther 2007, 9 - 10.)

Virtuaalilinkkien luominen

Oletetaan, että PE-a kuuluu VPLS:een foo ja luo mainostuksen VE ID:llä V, VE Block Offset:llä VBO, VE Block Size:llä VBS ja Label Base:llä LB. PE-b kuuluu myös VPLS:een foo ja sillä on VE ID:nä W. PE-b tekee seuraavat toimenpiteet saatuaan mainostuksen PE-a:lta (Kompella & Rekther 2007, 10.):

1. Tarkistaa kuuluuko W PE-a:n Remote VE Set -attribuuttiin: jos VBO <= W < VBO + VBS, silloin W kuuluu PE-a:n kanssa samaan VPLS:een. Mikäli näin ei ole PE-b hylkää viestin ja hyppää lopun proseduurista yli.
2. Luo virtuaalilinkin PE-a:han: leima, jota käytetään liikenteen lähettämiseen PE-b:ltä PE-a:lle, lasketaan seuraavalla kaavalla: LB + W – VBO.
3. Tarkistaa kuuluuko V mihinkään Remote VE Set -attribuuttiin, joita PE-b mainostaa. PE-b tarkistaa siis kuuluuko V johonkin Remote VE Set -attribuuttiin, joita PE-b mainostaa. Esim. VE Block Offset:lla VBO', VE Block Size:llä VBS' ja Label Base:lla LB'.
4. Luo virtuaalilinkin PE-a:sta: leima, jota käytetään liikenteen vastaanottamiseen PE-a:lta, lasketaan seuraavalla kaavalla: *LB' + V – VBO'*.

PE-a:n täytyy purkaa oman puolen virtuaalilinkki PE-a:n ja PE-b:n välillä, mikäli PE-b hylkää V:n sisältämän NLRI:n.

PE-laitteiden ominaisuuksien signalointi

Layer 2 Info Extended Comminity -kehystä käytetään signaloimaan kontrolli-informaatiota virtuaalilinkeistä. Kuviossa 24 on L2-tason Extended Community -informaatiokehys. Kontrolli-informaatio sisältää Encaps Type:n (virtuaalilinkkien käyttämän kapselointitavan), Control Flags:n (virtuaalilinkkien hallintaliput) ja Maximum Transmission Unit:n (MTU, virtuaalilinkin suurin mahdollinen pakettikoko). Encaps Type 19 on määritetty käytettäväksi VPLS:ssä. (Kompella & Rekther 2007, 11.)

Extended Comminity Type (16 bittiä)
Encaps Type (8 bittiä)
Control Flags (8 bittiä)
Layer-2 MTU (16 bittiä)
Reserved (16 bittiä)

KUVIO 24. L2-tason Extended Community -informaatiokehys

BGP-signaloidun VPLS:n toiminta

Verkon hallintahenkilöstön konfiguroidessa uutta VPLS:ä, esim. VPLS foo, täytyy heidän valita Route-Target (esim. RT-foo) kyseiselle VPLS:lle. Tätä RT:n arvoa käytetään kaikissa PE-laitteissa, jotka palvelevat VPLS foo:ta. PE-a:ta konfiguroitaessa osaksi VPLS foo:ta, täytyy hallintahenkilöstön ainoastaan valita VE ID (esim. V). PE-laiteelle voidaan myös konfiguroida Route Distinguisher (RD), esimerkiksi RD-foo. Mikäli RD:tä ei manuaalisesti konfiguroida, PE-laite generoi uniikin RD:n VPLS foo:lle. PE-a-laite generoi tämän jälkeen leimaryhmän ja Remote VE Set -attribuutin V:lle, mikä määritellään VE Block Offset:llä VBO, VE Block Size:llä VBS ja Label Base:lla LB. (Kompella & Rekther 2007, 11 - 12.)

PE-a-laite luo VPLS:n BGP NLRI -paketin seuraavilla arvoilla:

- RD = RD-foo-a
- VE ID = V
- VE Block Offset = VBO
- VE Block Size = VBS
- Label Base = LB

Ylläoleviin arvoihin PE-a-laite liittää L2 tason Extended Community -informaatiokehyksen ja Route-Target:n RT-foo. PE-a-laite määrittää BGP Next Hop -kenttään itsensä ja mainostaa tätä NLRI-pakettia naapureilleen.

Jos PE-a vastaanottaa VPLS:n BGP-mainoksen arvoilla RT-foo ja VE ID:n arvolla W, joltain muulta PE-laitteelta, esimerkiksi PE-b:ltä, tietää PE-a, että PE-b kuuluu samaan VPLS:een. Tässä toteutuu BGP-signaloinnin Auto Discovery -ominaisuus. Tämän jälkeen PE-a:n täytyy luoda oma osuutensa virtuaalilinkistä PE-a:n ja PE-b:n välillä. PE-b-laite toimii vastaavasti. Näin signalointi ja virtuaalilinkkien luonti saavutettiin yhdellä päivitysviestillä. (Kompella & Rekther 2007, 12.)

PE-b-laite ei pysty luomaan omaa osuuttaan virtuaalilinkistä, jos VE ID:n arvo W ei ole osa PE-b:n mainostamaa Remote VE Set -attribuuttia. Tähän ratkaisuna PE-a voi perua edellisen mainostuksen, jonka se teki VPLS foo:lle, ja mainostaa uutta päivitys-

viestiä, jossa on suurempi Remote VE Set -attribuutin arvo ja leimaryhmä, joka kattaa kaikki VE ID:t VPLS:ssä foo. Vaihtoehtoisesti PE-a voi luoda uuden Remote VE Set -attribuutin ja leimaryhmän sekä mainostaa näitä uudessa päivitysviestissä ilman edellisien mainosviestien perumista. (Kompella & Rekther 2007, 12.)

PE-a-laitteen täytyy perua kaikki mainosviestit, mikäli sen VPLS:n foo konfiguraatiosta poistetaan VE ID:n arvo V. Jos kaikki PE-a:n linkit CE-laitteisiin menevät pois käytöstä, täytyy PE-a:n joko perua kaikki sen lähettämät NLRI:t VPLS:lle foo tai ilmaista muille PE-laitteille jollakin tavalla, ettei se enää ole yhteydessä PE-a:han kytkettyihin CE-laitteisiin. (Kompella & Rekther 2007, 12.)

6.4 VPLS käyttäen LDP-signalointia

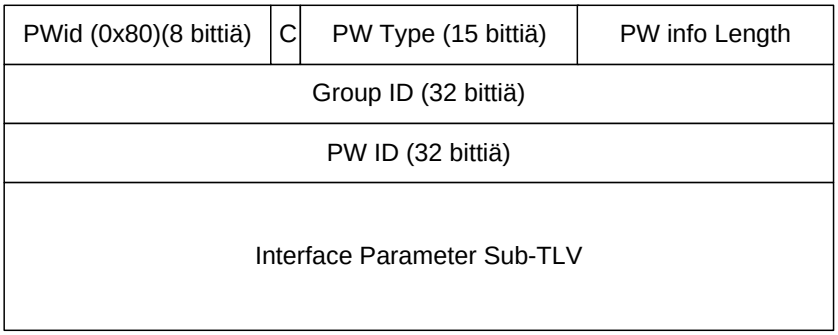
RFC 4447 määrittelee virtuaalilinkkien LDP-signaloinnin, mihin myös RFC 4762:ssa viitataan. LDP-signalointi vaatii täysin kytketyn verkon LDP-istuntoja, joita käytetään muodostamaan virtuaalilinkkejä. PE-laite tarvitsee VPLS:n LDP-signalointietojen välittämiseen olemassa olevaa LDP-istuntoa toiseen PE-laitteeseen. LDP-istuntoa käytetään kaikkien virtuaalilinkkien muodostamiseen ja parametrien välittämiseen näiden kahden PE-laitteen välillä.

LDP-signaloinnissa käytetään LDP Label Mapping -viestejä, jotka sisältävät FEC TLV:n, Label TLV:n ja ei yhtään tai useamman Parameter TLV:n. FEC TLV:tä käytetään osoittamaan leiman tarkoitus. FEC TLV:stä käy ilmi tietty virtuaalilinkki, johon kyseinen leima viittaa. FEC TLV:n eli tietovuon Type-Length-Value-koodauksen muodostamiseen on RFC 4447:ssä määritetty kaksi erilaista viestityyppiä: PWid FEC Element (tietovuon tyyppi on 128) ja Generalized PWid FEC Element (tietovuon tyyppi on 129). RFC 4762:n mukaan ei suositella käytettäväksi PWid FEC Element-viestejä, mutta sen mukaisia implementaatioita on laitevalmistajilla vielä käytössä. Virtuaalilinkin muodostamisessa ei käytetä kuin toista edellä mainituista FEC Element:stä. (El-Aawar, Heron, Martini, Rosen & Smith 2006, 7 – 8; Kompella & Lasserre 2007, 8.)

PWid FEC Element -kehys

Kuviossa 25 on esitetty PWid FEC Element -kehys, jossa on seuraavat kentät:

- PWid, joka määrittää tietovuon Element-tyypin.
- C, joka on Control Word Bit, määrittää Control Word:n olemassa oloa.
- PW Type, joka on 15 bittinen arvo, jolla määritetään virtuaalilinkin tyyppi.
- PW Information Length määrittää PW ID-kentän pituuden. Mikäli tämän kentän arvo on 0, silloin kaikkiin virtuaalilinkkeihin viitataan tietyllä Group ID:llä.
- Group ID on 32-bittinen arvo, joka määrittää mielivaltaisen arvon joukolle virtuaalilinkkejä, jotka muodostavat tietyn joukon virtuaalilinkkejä.
- PW ID on 32-bittinen arvo, joka määrittää yhdessä PW Type-arvon kanssa tietyn virtuaalilinkin.
- Interface Parameter Sub-TLV:n avulla välitetään rajapintakohtaisia määrityksiä.



KUVIO 25. PWid FEC Element -kehys

Generalized PWid FEC Element -kehys

Kuviossa 26 on esitetty Generalized PWid FEC Element -kehys, joka on siis nykyään RFC 4762:ssa suositeltu kehystyyppi. Kehyksen C ja PW Information Length -kentät ovat samat kuin PWid FEC Element -kehyksessä. PWid-arvo on Generalized PWid FEC Element -kehyksen tapauksessa 0x81. PW Type -kentässä arvot voivat olla VPLS:n tapauksessa ainoastaan joko 0x0005 Ethernet-kehyksille tai 0x004 leimatuille Ethernet-kehyksille. PWid FEC Element -kehys ei sisällä lainkaan Group ID -kenttää,

mutta sitä vastaava toiminnallisuus on toteutettavissa LDP:n PW Grouping TLV -kehyksellä. (Kompella & Lasserre 2007, 8.)

AGI eli Attachment Group Identifier TLV kuvaa VPLS:n nimen tyypin Type-kentässä, Value-kentän pituuden Length-kentässä ja Value-kentässä on kyseisen VPLS:n nimi. AGI:a kutsutaan yleisesti myös VPLS-tunnisteeksi. (Kompella & Lasserre 2007, 8.)

TAII eli Target Attachment Individual Identifier- ja SAII eli Source Attachment Individual Identifier -kentät ovat nollia, koska kytketyt virtuaalilinkit VPLS:ssä päättyvät MAC-tauluihin, eikä itsenäisiin asiakasliityntöihin. TAII- ja SAII-kentät ovat varattu tulevaisuuden parannuksia varten. (Kompella & Lasserre 2007, 8.)

Gen PWid (0x81)	C	PW Type (15 bittiä)	PW info Length
AGI Type	Length	Value	
AGI Value			
AII Type	Length	Value	
SAII Value			
AII Type	Length	Value	
TAII Value			

KUVIO 26. Generalized PWid FEC Element -kehys

LDP-signaloinnin toiminta

PE-laitteen (PE-A) tarvitsee tietää toisen PE-laitteen (PE-B) osoite sekä VPLS-tunniste, jotta se voi aloittaa VPLS-signaloinnin laitteiden välillä. Nämä tiedot voi olla joko konfiguroituna laitteeseen tai ne on opittu jonkin Auto Discovery -toiminnon kautta. Lähettävä laite PE-A aloittaa virtuaalilinkin luomisen lähettämällä Label Mapping -viestin vastaanottavalle laitteelle PE-B. Label Mapping -viestissä on sisällä Generalized PWid FEC Element -kehys. PE-B:n vastaanotettua viestin, se tulkitsee viestin ja aloittaa virtuaalilinkin muodostamisen omassa päässään. Virtuaalilinkkiä ei voida muodostaan molempiinsuuntiin ellei virtuaalilinkki polkua ole olemassa laitteiden välillä. Mikäli toinen suunta on jo olemassa, voi PE-B lähettää uuden Label Mapping -viestin, jonka avulla muodostetaan virtuaalilinkki toiseen suuntaan. (El-Aawar, Heron, Martini, Rosen & Smith 2006, 14 - 15.)

LDP-signaloinnin luotua virtuaalilinkin PE-laitteiden välille, voidaan asiakkaan Ethernet-kehykset kapseloida ja kuljettaa luotua virtuaalilinkkiä pitkin toiseen PE-laitteeseen ja edelleen siihen kytkettyyn asiakaslaitteeseen. Jos asiakkaan liikenteen leimaamiseen käytetään VLAN-leimoja liityntäverkossa (esimerkiksi QinQ-leimoja), ne voidaan joko poistaa kehyksen tullessa PE-laitteeseen ja kuljettaa ilman leimatietoa MPLS-verkon läpi tai leima säilytetään kehyksessä koko sen kulkeman matkan verkossa. Toisaalta, jos kehys sisältää asiakkaan omia VLAN-leimoja, niitä ei poisteta vaan ne kulkevat kehyksen mukana päätepisteeseen asti. (Kompella & Lasserre 2007, 11 - 12.)

Osoitteiden oppiminen VPLS-palvelua käytettäessä tapahtuu L2-tason osoitetietojen perusteella Forwarding Information Base:ssa (FIB) eli kytkentätaulussa. Kytkentätaulu ylläpitää tietoa MAC-osoitteiden ja virtuaalilinkkien vastaavuuksista. On olemassa kahden tyyppistä oppimista: varauksellinen (qualified) ja varaukseton (unqualified). Varauksellinen oppimistapa on oletustoiminto ja se pitää olla tuettuna. Varauksettomassa oppimistavassa asiakkaan kaikki VLAN:t ovat yhdessä VPLS-instanssissa, mikä tarkoittaa, että ne jakavat yhden yhteisen yleislähetysalueen sekä yhden yhteisen MAC-osoitetaulun. Varauksellisessa oppimistavassa jokainen asiakkaan VLAN liitetään omaan VPLS-instanssiin, mikä tarkoittaa, että jokaisella VLAN:lla on oma yleislähetysalue ja oma MAC-osoitetaulu. (Kompella & Lasserre 2007, 12 - 13.)

7 BORDER GATEWAY PROTOCOL (BGP)

7.1 Yleistä

Border Gateway Protocol (BGP) on alueiden välinen reititysprotokolla, mikä tarkoittaa, että se toimii eri hallinnassa olevien verkkojen välillä. BGP on siis ulkoinen reititysprotokolla (Exterior Gateway Protocol) eli sitä käytetään pääsääntöisesti mm. eri autonomisten alueiden (Autonomous System, AS) väliseen reittitietojen vaihtamiseen. BGP on polkuvektori reititysprotokolla, joka käyttää AS-numeroiden sarjaa kuvaamaan reittiä tiettyyn verkkoon. BGP:n välittämä reittitieto on pelkästään verkko-osoite (esim. 130.234.0.0/16), johon on liitetty AS_Path-attribuutti, jonka perusteella selviää käytettävä polku kyseiseen verkkoon. BGP on reititysprotokollista ainoa, joka käyttää luotettavaa TCP-protokollaa hallinta- ja päivitysviestien välittämiseen naapuruuksien välillä. Luotettavan siirtoprotokollan käyttäminen tarkoittaa, ettei jaksollisia päivityksiä tarvita. Tämä on välttämätöntä, koska nykyisellään täysi Internet BGP-taulu sisältää yli 300 000 BGP-reittitietoa. BGP kuitenkin generoi säännöllisiä keepalive-viestejä, joiden avulla se varmistaa, että käytettävä TCP-yhteys on toiminnassa. BGP kuuntelee TCP-protokollan porttia 179. (Marschke & Reynolds 2008, 200 – 201; Hares, Li & Rekhter 2006, 7 - 8.)

BGP-viesteissä käytetään parametrien tyyppi, pituus ja arvo (Type-Length-Value, TLV) joukkoa kuvaamaan välitettävän viestin sisältöä. TLV:den käyttö mahdollistaa uusien ominaisuuksien tuomisen BGP:hen ilman tarvetta tehdä suuria muutoksia protokollaan, esimerkiksi IPv6-protokollalle luotiin uusi NLRI-attribuutti, joka mahdollisti IPv6-reittitietojen välittämisen BGP:n avulla. (Marschke & Reynolds 2008, 201.)

BGP:stä on olemassa kaksi erillistä yhteystyyppiä, eBGP ja iBGP. eBGP:n ja iBGP:n eroavaisuuksia on listattu taulukossa 1. iBGP:tä käytetään reitittämään liikennettä autonomisen alueen sisällä. iBGP:tä voidaan käyttää signalointiprotokollana useille eri verkkoprotokollille kuten esimerkiksi VPLS:lle ja MPLS-VPN:lle. iBGP-protokollaa käytettäessä luodaan saman AS:n sisällä naapuruus reitittimien välille, joiden halutaan vaihtavan signalointi- tai reittitietoja. eBGP reitittää liikennettä rinnakkaisten AS:n välillä. Jokainen AS ylläpitää omaa reititystaulua ja -politiikkoja. Internet-reititykseen

osallistuvien reitittimille pitää kuulua johonkin autonomiseen alueeseen. AS-numerot on alunperin muodostettu 16-bittisestä arvosta ja ne voivat olla 1 - 65535 välillä. Yksityisille AS:lle on varattu arvot väliltä 64512 - 65535. Nykyään Internetin kasvamisen johdosta on AS-numeroiden määrä kasvatettu 32-bittiseksi arvoksi eli eri AS-numeroiden määrä on yli neljä miljardia kappaletta. Uusi merkkaustapa on x.y. Käytettäessä uutta merkkaustapaa vanhat AS-numerot merkataan 0.y, jossa on y on vanhan merkkaustavan mukainen AS-numero.

TAULUKKO 1. eBGP:n ja iBGP:n eroavaisuudet

Ominaisuus/attribuutti	**iBGP**	**eBGP**
Paikallinen AS-numero lisätään AS-polkuun	Ei	Kyllä
Next Hop -attribuutti korvataan	Ei	Kyllä
Uusi MED-attribuutti lisätään	Ei. eBGP:n kautta vastaanotettu MED-attribuuttia voidaan mainostaa iBGP:tä käyttäen AS:n sisällä	Kyllä
Local Preferece -attribuutti	Kyllä	Ei
Naapuruusosoite	Yleensä loopback-osoite, käytetään IGP-protollan reittitietoja (TTL=64)	Yleensä naapuus muodostetaan liitettyyn rajapintaan (TTL=1)
eBGP:n kautta vastaanotettu päivitys lähetetään	Kaikille iBGP-naapureille	Muille eBGP-naapuruuksille
iBGP:n kautta vastaanotettu päivitys lähetetään	Ei iBGP-naapureille	Kaikille eBGP-naapuruuksille

iBGP-päivitykset eivät muuta AS Path -attribuuttia, josta seuraa silmukoiden mahdollisuus. Tästä syystä iBGP-reitittimet eivät voi mainostaa toiselta iBGP-reitittimeltä opittuja reittejä eteenpäin iBGP-naapurille, mistä seuraa vaatimus, että iBGP-reitittimet pitää olla täysin kytkettyjä toisiinsa. Next Hop -attribuutin käsittelyn eroavaisuudet usein johtavat näkymättömiin iBGP-reitteihin, koska reititin ei osaa selvittää

reittiin yhdistettyä seuraavaa BGP-hyppyä. Oletuksena seuraava BGP-hyppy identifioi eBGP-naapurin IP-osoitteen. MED-attribuutti normaalisti lisätään reittipäivitykseen ainoastaan, kun reittiä mainostetaan eBGP:llä. Local Preference -attribuuttia käytetään ainoastaan iBGP-päivitysviesteissä. Naapuruuksien luomisen eroavaisuudet ovat merkittäviä useasta syystä. eBGP normaalisti muodostaa naapuruuden käyttäen suoraan kytketyn liitynnän osoitetta, mistä seuraa ettei rekursiivista reititystä tarvitse tehdä vaan reitittimen reittitaulussa on jo tieto mitä rajapintaa käyttäen ko. osoite löytyy. Tietoturvasyistä paketin elinikä (TTL) on oletuksena asetettu eBGP-istunnoille ykköseksi. iBGP:ssä käytetään yleisesti naapuruuden muodostamisessa loopback-rajapinnan osoitetta. Tämän ansiosta iBGP-istunto ei välttämättä katkea yhden rajapinnan rikkoutumisen tms. takia. iBGP turvautuu IGP-protokollaan etsiessään reittiä naapurireitittimeen. (Marschke & Reynolds 2008, 208 - 209.)

7.2 BGP-viestityypit

BGP käyttää sarjaa viestejä BGP-istuntojen aloittamiseen, aktiivisuuden varmistamiseen, reittipäivitysten lähettämiseen ja ilmoittamaan naapurireitittimille virhetiloista. Jokaista näistä viesteistä käytetään tietyn tyyppiseen toimintoon. Taulukossa 2 on yhteenveto viesteistä, joita käytetään kaikissa BGP-istunnoissa.

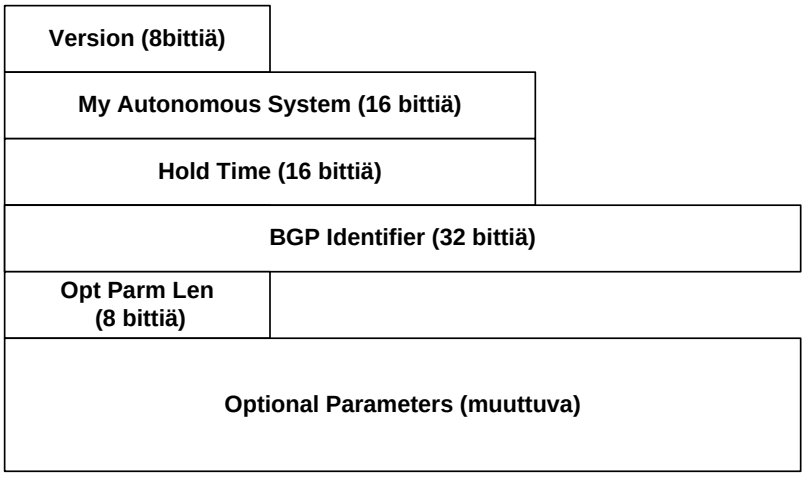
TAULUKKO 2. BGP-viestityypit

Viestinumero	Viestityyppi	Viestin kuvaus
1	OPEN	Käytetään avaamaan BGP-istunto
2	UPDATE	Kuljettaa reittipäivitykset muodostettujen BGP-istuntojen välillä
3	NOTIFICATION	Ilmoittaa BGP-istunnon toiselle osapuolelle virhetilanteesta
4	KEEPALIVE	Käytetään varmistamaan BGP-istunnon aktiivisuus
5	ROUTE-REFRESH	Valintainen viesti, joka lähetään, kun halutaan dynaamisia BGP reittipäivityksiä BGP-naapurilta.

Taulukossa 2 näkyvät viestityypit auttavat BGP-osapuolia etenemään eri BGP-tilojen välillä. Molempien BGP-osapuolten saavutettua Established-tila, aloittavat ne vaihtamaan reittipäivityksiä. Ensimmäisessä reittipäivitysviestissä vaihdetaan koko reittitaulun sisältö, minkä jälkeen päivitykset sisältävät vain reittimuutokset (lisäyksen, muutoksen tai reitin poistamisen). BGP-istunnon katkettua, BGP-prosessi välittömästi lopetetaan ja kaikki reitit, jotka on opittu BGP-istunnon kautta poistetaan reittitaulusta.

OPEN-viesti

BGP-osapuolien välille tarvitsee ennen BGP-istunnon aloittamista olla luotuna TCP-yhteys, kun se on muodostettu ensimmäiset OPEN-viestit lähetetään molempien osapuolien toimesta. BGP-osapuoli vastaa viestiin KEEPALIVE-viestillä, jos se hyväksyy OPEN-viestin. Kuviosta 27 on nähtävissä OPEN-viestin kentät. OPEN-viesti sisältää paikallisen BGP-osapuolen tietoja. (Hares, Li & Rekhter 2006, 13.)



KUVIO 27. OPEN-viesti (Hares, Li & Rekhter 2006, 13)

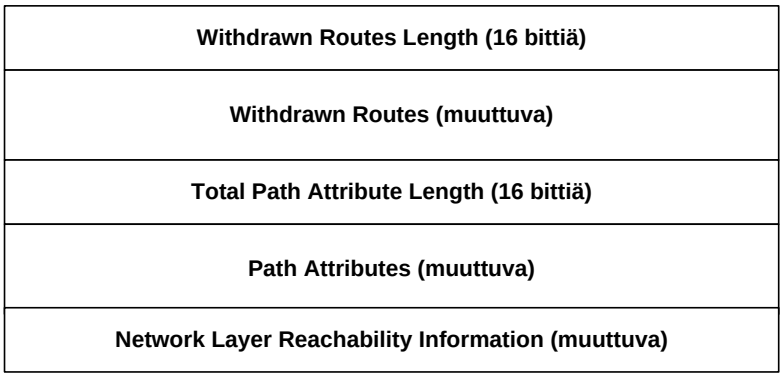
Taulukossa 3 on kuvattu OPEN-viestin eri kenttien merkitys.

TAULUKKO 3. OPEN-viestikenttien kuvaukset (Hares, Li & Rekhter 2006, 13 - 14)

Kenttä	**Kuvaus**
Version	Käytettävä BGP-versio
My Autonomous System	AS-numero, joka on käytössä BGP-osapuolella
Hold Time	Kertoo ajan pituuden, jonka BGP-osapuoli odottaa Update- tai Keepalive-viestiä ennen istunnon purkamista. Hold Time:n pitää olla molemmilla osapuolilla sama, jotta istunnon muodostaminen etenee
BGP Identifier	BGP-osapuolen 32-bittinen tunniste
Optional Parameters	Sisältää valinnaisia BGP-parametrejä, kuten esimerkiksi Marker-kenttä, joka sisältää autentikointitietoa

UPDATE-viesti

BGP-osapuolet aloittavat vaihtamaan reittitietoja käyttäen UPDATE-viestejä, kun BGP-istunto on muodostettu eli sen tila on Established. UPDATE-viesti sisältää tietoa reitistä, jota mainostetaan toiselle BGP-osapuolelle. BGP-reitityksessä verkko-osoitteita kutsutaan myös Network Layer Reachability Information:ksi (NLRI). Kuviossa 28 on UPDATE-viestin kentät.



KUVIO 28. UPDATE-viesti (Hares, Li & Rekhter 2006, 15)

Taulukossa 4 on esitetty UPDATE-viestin kenttien kuvaukset.

TAULUKKO 4. UPDATE-viestikenttien kuvaus (Hares, Li & Rekhter 2006, 15 - 16)

Kenttä	**Kuvaus**
Withdrawn Routes Length	Ilmoittaa seuraavan kentän pituuden
Withdrawn Routes	Sisältää kaikki reittitiedot, jotka poistetaan BGP-taulusta
Total Path Attribute Length	Ilmoittaa seuraavan kentän pituuden
Path Attributes	BGP-polkuattribuutit ovat periaatteessa BGP-reitin ominaisuuksia, joita käytetään määrittelemään reitin paremmuus. IANA on määritellyt yhteensä 19 attribuuttia. Polkuattribuutit erotellaan toisistaan koodien perusteella. Attribuutit ovat kuvattu kappaleessa 7.2
Network Layer Reachability Information	Sisältää reitit, jotka mainostetaan saavutettaviksi. Kenttä sisältää verkko-osoitteet jokaiselle polulle, joita mainostetaan toiselle BGP-osapuolelle

KEEPALIVE-viesti

BGP ei käytä mitään TCP-pohjaista ylläpitoviestiä varmistaakseen onko BGP-osapuoli saavutettavissa. KEEPALIVE-viestejä vaihdetaan BGP-osapuolien välillä tarpeeksi usein, ettei Hold Time -ajastin ehdi täyttyä. KEEPALIVE-viestien väli tulisi olla 1/3 Hold Time -ajastimen arvosta. KEEPALIVE-viesti sisältää ainoastaan viestiotsikon, jolla on pituutta 19 oktettia.

NOTIFICATION-viesti

NOTIFICATION-viestejä käytetään ilmoittamaan virhetilanteesta, joka aiheuttaa välittömän BGP-istunnon purkamisen. BGP-yhteyden purkamisen jälkeen TCP-istunto BGP-osapuolien välillä ajetaan alas, kaikki resurssit vapautetaan, Route Withdrawal -viestit lähetetään BGP-osapuolille ja kaikki BGP-reitit poistetaan reittitaulusta. Kuvissa 29 on esitetty NOTIFICATION-viesti.

Error Code (8 bittiä)	Error Subcode (8 bittiä)	Data (muuttuva)

KUVIO 29. NOTIFICATION-viesti (Hares, Li & Rekhter 2006, 22)

Taulukossa 5 on kuvattu kuusi merkittävintä NOTIFICATION-virhekoodia.

TAULUKKO 5. NOTIFICATION-viestin virhekoodit (Hares, Li & Rekhter 2006, 22)

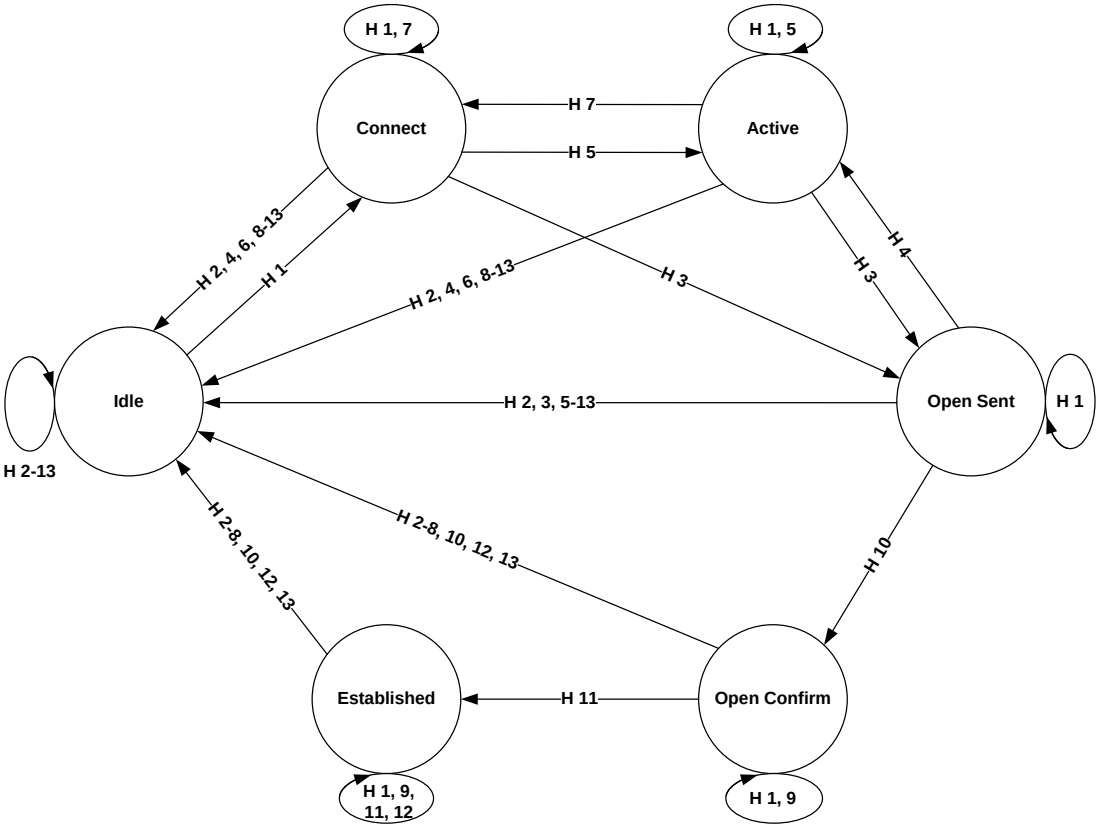
Virhekoodi	**Viestityyppi**	**Kuvaus**
1	Message Header -virhe	Ilmoitetaan löytyneestä virheestä BGP-viestiotsikkoa prosessoidessa
2	OPEN-viestivirhe	Ilmoitetaan löytyneestä virheestä OPEN-viestissä
3	UPDATE-viestivirhe	Ilmoitetaan löytyneestä virheestä UPDATE-viestissä
4	Hold Timer-ajastin on täyttynyt	Tämä virheilmoitus lähetetään, kun BGP-osapuoli ei ole vastaanottanut KEEPALIVE- tai UPDATE-viestejä Hold Time-ajan sisällä.
5	Tilakonevirhe	Tilakone virhe lähetetään, kun odottamaton virhe ilmaantuu.
6	Cease	Välitön BGP-istunnon päättäminen

Lisäksi on olemassa joukko alivirhekoodeja, jotka tarkentavat merkittävien virheilmoitusten sisältöä.

7.3 BGP:n tilakoneen toiminta

BGP-osapuolet vaihtavat tiloja useaan kertaan ennen kuin muodostavat naapuruuden ja aloittavat reittitietojen vaihtamisen. Jokaisen tilan aikana BGP-osapuolten täytyy lähettää ja vastaanottaa viestejä, käsitellä viestidataa ja alustaa resurssit ennen siirtymistä seuraavaan tilaan. Tätä prosessia voidaan kuvata BGP-tilakoneen avulla. Kuviossa 30 ja taulukossa 6 on kuvattuna BGP-tilakoneen tilat ja herätteet, jotka aiheuttavat vaihtumisen tilojen välillä (DeHaven Carroll & Doyle 2001, 95). Jos prosessi epäonnistuu jossain kohtaa, istunto lopetetaan ja molemmat osapuolet palaavat Idle-tilaan ja aloittavat prosessin alusta. BGP-osapuolet vaihtavat jatkuvasti eri tilojen välillä, mikäli jomman kumman osapuolen konfiguraatioissa on vikaa. BGP-osapuolet vaihtavat läpi seuraavien tilojen ennen kuin ne voivat muodostaa BGP-istunnon:

- Idle
- Connect
- Active
- Open Sent
- Open Conform
- Established



KUVIO 30. BGP-tilakone (DeHaven Carroll & Doyle 2001, 95)

TAULUKKO 6. BGP-tilakoneen herätteet (Lynch & Solie 2003, 554 - 555)

Heräte	**Herätteen nimi**	**Kuvaus**
1	BGP Start	Tapahtuu Idle-tilan aikana. BGP Start -heräte aloittaa BGP-istunnon muodostamisen. Herätettä odotetaan ainoastaan Idle-tilassa
2	BGP Stop	BGP Stop -heräte ilmoittaa BGP-istunnon purkamisesta
3	BGP Transport Connection Open	Heräte ilmoittaa osapuolelle, että TCP-yhteys on auki
4	BGP Transport Connection Closed	Heräte ilmoittaa osapuolelle, että toinen BGP-osapuoli on sulkenut TCP-istunnon.
5	BGP Transport Connection Failed	Heräte ilmoittaa, että TCP-yhteys toiseen osapuoleen on epäonnistunut.
6	BGP Transport Fatal Error	Heräte ilmoittaa, että TCP-istunnossa on tapahtunut tuhoisa virhe
7	ConnectRetry-ajastin vanhentui	Herätä tapahtuu kun ConnectRetry-ajastin vanhentuu. Kun ajastin vanhentuu se uudelleenkäynnistetään
8	Hold Timer -ajastin vanhentui	Heräte tapahtuu, kun Hold Timer -ajastin vanhentuu. Tarkoittaen, että toinen osapuoli ei ole vastannut viestiin paikalliselta osapuolelta.
9	KEEPALIVE Timer -ajastin vanhentui	Heräte ilmoittaa, että KEEPALIVE-ajastin on vanhentunut, viestittäen ettei toiselta osapuolelta ole saatu KEEPALIVE-viestejä Hold Timer -ajastin puitteissa
10	Vastaanotettiin OPEN-viesti	Heräte ilmoittaa, että OPEN-viesti on vastaanotettu toiselta osapuolelta. BGP-istunto voi siirtyä OpenConfirm-tilaan.
11	Vastaanotettiin KEEPALIVE-viesti	Heräte ilmoittaa, että KEEPALIVE-viesti on vastaanotettu ja BGP-istunto voi siirtyä Established-tilaan.
12	Vastaanotettiin UPDATE-viesti	Heräte ilmoittaa, että on vastaanotettu UPDATE-viesti
13	Vastaanotettiin NOTIFICATION-viesti	Heräte ilmoittaa, että NOTIFICATION-viesti on vastaanotettu ja BGP-istunto tulisi purkaa välittömästi

Idle-tila

BGP aloittaa aina toimintansa Idle-tilasta, jossa se hylkää kaikki tulevat yhteydet. Heräte 1:n tapahtuessa BGP-prosessi alustaa kaikki BGP-resurssit, käynnistää Connect-Retry-ajastimen, aloittaa TCP-yhteyden toiseen BGP-osapuoleen, kuuntelee TCP-yhteyden aloitusta BGP-osapuolelta ja vaihtaa tilan Connect-tilaan. Start-heräte käynnistyy BGP-prosessin konfiguroinnista, olemassa olevan prosessin uudelleenkäynnistämisestä tai reitittimen ohjelmiston uudelleenkäynnistäessä BGP-prosessi. Virhe palauttaa BGP-prosessin Idle-tilaan. Tästä eteenpäin reititin voi automaattisesti käynnistää Start-herätettä, mutta sen voi käynnistää vasta ConnectRetry-ajastimen vanhennuttua. (DeHaven Carroll & Doyle 2001, 96.)

Connect-tila

Connect-tilassa BGP-prosessi odottaa TCP-yhteyden valmistumista. Jos TCP-yhteys onnistuu, BGP-prosessi tyhjentää ConnectRetry-ajastimen, lopettaa alustamisen, lähettää OPEN-viestin ja siirtyy Open Sent -tilaan. BGP-prosessi jatkaa kuuntelua TCP-yhteydelle, nollaa ConnectRetry-ajastimen ja siirtyy Active-tilaan, mikäli TCP-yhteys ei onnistu. Jos ConnectRetry-ajastin vanhenee, BGP-prosessi pysyy Connect-tilassa, nollaa ajastimen ja tekee uuden yrityksen muodostaakseen TCP-yhteyden. Mikä tahansa muu heräte siirtää BGP-prosessin Idle-tilaan. (DeHaven Carroll & Doyle 2001, 97.)

Active-tila

Active-tilassa BGP-prosessi yrittää aloittaa TCP-yhteyden BGP-naapurin kanssa. Jos TCP-yhteys onnistuu, BGP-prosessi nollaa ConnectRetry-ajastminen, lopettaa alustuksen, lähettää OPEN-viestin BGP-naapurille ja siirtyy Open Sent -tilaan. Mikäli ConnectRetry-ajastin vanhenee, kun BGP-prosessi on Active-tilassa, se siirtyy takaisin Connect-tilaan ja nollaa ConnectRetry-ajastimen. Prosessi myös alustaa TCP-yhteyden toiseen BGP-osapuoleen ja jää odottamaan TCP-yhteyttä.Mikä tahansa muu heräte (paitsi Start-heräte, jota ei huomioida Active-tilassa) aiheuttaa tilan siirtymisen Idle-tilaan. (DeHaven Carroll & Doyle 2001, 97.)

Open Sent -tila

Tähän tilaan tultaessa OPEN-viesti on jo lähettetty ja BGP-prosessi odottaa vastaanottavansa OPEN-viestin BGP-naapuriltaan. Kun OPEN-viesti vastaanotetaan, kaikki sen kentät tarkistetaan ja virhe havaittaessa lähetetään NOTIFICATION-viesti ja tila siirtyy Idle-tilaan. KEEPALIVE-viesti lähetään ja asetetaan KEEPALIVE-ajastin, jos virheitä ei havaittu. Hold Time -ajastin neuvotellaan ja sovitaan käytettäväksi pienempää arvoa paitsi jos arvo on nolla, jolloin Hold Time- ja KEEPALIVE-ajastimia ei käynnistetä. BGP-osapuoli määrittelee onko kyseessä sisäinen vai ulkoinen BGP-prosessi perustuen AS-numeroon ja siirtyy sen jälkeen Open Confirm -tilaan. BGP-prosessi sulkee BGP-yhteyden, nolla ConnectRetry-ajastimen, aloittaa kuuntelemaan uusia yhteyksiä ja siirtyy Active-tilaan, jos TCP-yhteys katkeaa. Mikä tahansa muu heräte (paitsi Start-heräte, jota ei huomioida Open Sent -tilassa) aiheutta tilan siirtymisen Idle-tilaan. (DeHaven Carroll & Doyle 2001, 97.)

Open Conform-tila

Tässä tilassa BGP-prosessi odottaa KEEPALIVE- tai NOTIFICATION-viestejä. Prosessi siirtyy Established-tilaan, jos KEEPALIVE-viesti saapuu. Mikäli NOTIFICATION-viesti saapuu tai TCP-yhteys katkeaa, prosessi siirtyy tila Idle-tilaan. Jos Hold Timer -ajastin vanhenee, virhe havaitaan, Stop-heräte tapahtuu, lähetetään NOTIFICATION-viesti BGP-naapurille ja BGP-yhteys suljetaan ja tila siirtyy Idle-tilaan. (DeHaven Carroll & Doyle 2001, 98.)

Established-tila

Tässä tilassa BGP-osapuolet ovat täysin muodostaneet BGP-istunnon ja osapuolet voivat aloittaa UPDATE-, KEEPALIVE- ja NOTIFICATION-viestien lähettämisen. Vastaanotettaessa UPDATE- tai KEEPALIVE-viestin Hold Timer -ajastin nollataan. NOTIFICATION-viesti vastaanotettaessa tila siirtyy Idle-tilaan. (DeHaven Carroll & Doyle 2001, 98.)

7.4 Attribuutit

7.4.1 Pakolliset Well-Known-attribuutit

Pakolliset Well-Known-attribuutit pitää olla tuettuja kaikkien BGP-osapuolien toimesta ja niiden täytyy olla mukana jokaisessa BGP-päivitysviestissä, jossa on mukana reittitietoja.

Origin-attribuutti

Origin-attribuutti kertoo reittipäivityksen lähteen. BGP käyttää Origin-attribuuttia yhtenä tekijänä määrittäessään parasta reittiä. Lähde voi olla joku seuraavista:

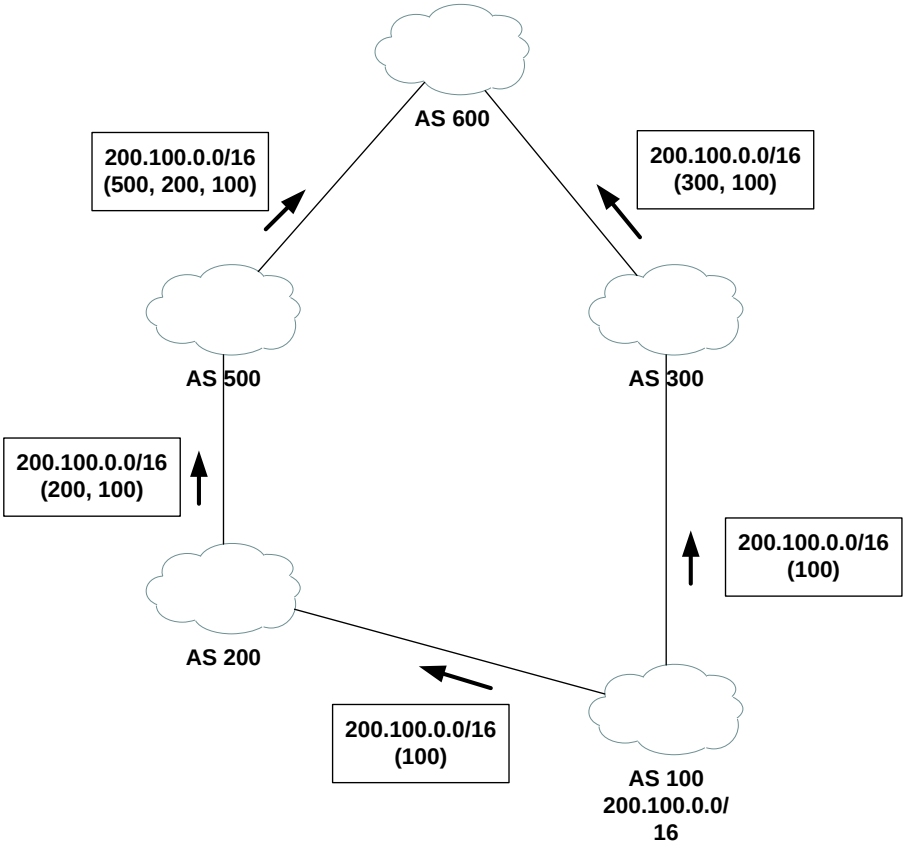
- IGP: BGP-reiteille annetaan Origin-attribuutin arvoksi IGP, jos ne on opittu sisäiseltä reititysprotokollalta.
- EGP: Reittitieto on opittu ulkoiselta reititysprotokollalta (EGP).
- Unknown / Incomplete: Reittitieto on opittu jollakin muulla tavalla. Unknown / Incomplete ei viittaa siihen, että reittitieto olisi jotenkin virheellinen vaan lähdettä ei ole pystytty määrittelemään. Esimerkiksi reittitiedot, jotka on opittu jakamalla (redistribute) jostakin toisesta protokollasta, saavat Origin-attribuutin arvoksi Unknow / Incomplete.

BGP:n käyttäessä Origin-attribuuttia määrittämään parasta reittiä, se suosii pienintä Origin-attribuutin arvoa: IGP < EGP < Unknown / Incomplete.

AS Path -attribuutti

AS Path -attribuutti sisältää sarjan AS-numeroita, jotka kuvaavat polun kyseisen reittitiedon saavuttamiseksi. AS Path -attribuuttia käytetään silmukoiden syntymisen estämiiseen ja se vaikuttaa myös reitin valintaan siten, että vähiten AS-numeroita sisältävän AS Path -attribuutin omaavaa reittitietoa suositaan. Jokainen autonominen alue lisää oman AS-numeronsa reittitietoon välittäessään ko. reittitietoa eteenpäin muille EBGP-naapureille. Oletuksena BGP-osapuoli hylkää kaikki reittimainokset, jotka sisältävät sen oman AS-numeron reittitiedon AS Path -attribuutissa. Tämä ominaisuus estää silmukoiden syntymisen.

Kuviossa 31 on esimerkki miten AS Path -attribuutti muuttuu reittitietoa välitettäessä eteenpäin. Jokainen autonominen alue lisää oman AS-numeron reittipäivitykseen, jota se välittää eteenpäin. Esimerkissä AS 100 lähettää molemmille naapureilleen (AS 200 ja AS 300) reittimainoksen (200.100.0.0/16), johon se on lisännyt oman AS-numeronsa. Kumpikin naapureista lähettää reittipäivitystä eteenpäin muille naapureilleen lisäten oman AS-numeron AS Path -attribuuttiin. Tämä toistuu myös AS 500 kohdalla. AS 600 vastaanottaa saman reittitiedon kahdella eri AS Path -attribuutin arvolla ja oletuksena se valitsee lyhimmän polun perusteella parhaan reitin 200.100.0.0/16-verkkoon ja lisää sen reittitauluunsa.



KUVIO 31. AS-polun muodostuminen

Next Hop -attribuutti

Next Hop -attribuutti kertoo sen BGP-osapuolen IP-osoitteen, mihin paketit pitäisi lähettää saavuttaakseen kyseisen reittitiedon. Next Hop -attribuutti vaihdetaan oletuk-

sena eBGP-reittipäivityksessä, mutta sitä ei vaihdeta iBGP-reittipäivityksessä. Tätä oletustoimintoa voidaan muuttaa eri valmistajien toteuttamilla toiminteilla.

7.4.2 Harkinnanvaraiset Well-Known-attribuutit

Local Preference -attribuutti

Local Preference -attribuuttia voidaan käyttää ainoastaan mainoksissa autonomisen alueen sisällä eli iBGP-osapuolien välillä. Attribuuttia käytetään määrittämään miten suositeltva kyseinen reittitieto on sitä lähettävän BGP-osapuolen näkökulmasta. Jos iBGP-osapuoli vastaanottaa useita reittejä samaan kohteeseen, se vertaa Local Preference -attribuuttia ja valitsee suurimman Local Preference -attribuutin omaavan reittitiedon laitettavaksi reititystauluun.

Atomic Aggregate -attribuutti

BGP-osapuoli voi lähettää päällekkäisiä reittitietoja toiselle BGP-osapuolelle. Päällekkäiset reitit eivät ole identtisiä reittejä, jotka osoittavat samaan kohteeseen. Esimerkiksi reitit 206.25.192.0/19 ja 206.25.128.0/17 ovat päällekkäisiä. Ensimmäinen reittitieto sisältyy jälkimmäiseen. Reitittimen tehdessä reitityspäätöksiä, se valitsee aina tarkimman reitin. BGP-osapuolella on useita vaihtoehtoja, kun se mainostaa päällekkäisiä reittejä:

1. Mainosta molemmat reitit
2. Mainosta ainoastaan tarkempi reitti
3. Mainosta ainoastaan ei päällekkäiset reitit
4. Yhdistä kaksi tai useampi reittitieto ja mainosta niitä
5. Mainosta ainoastaan vähemmän tarkkaa reittiä
6. Älä mainosta kumpaakaan

Atomic Aggregate -attribuuttia käytetään viestittämään naapurireitittimille, että reittitiedon tarkkuutta ollaan hävitetty. Aina kun BGP-osapuoli yhdistää tarkempia reittitietoja vähemmän tarkkoihin reittitietoihin (viides vaihtoehto ylläolevassa listassa), sen tarvitsee lisätä Atomic Aggregate -attribuutti yhdistettyyn reittitietoon. Muiden BGP-

osapuolien mainostaessa reittitietoa eteenpäin on Atomic Aggregate -attribuutti säilytettävä mukana reittimainostuksissa.

7.4.3 Valintaiset Transitive-attribuutit

Aggregator-attribuutti

BGP-osapuoli voi lisätä myös Aggregator-attribuutin mainosviestiin, mikäli Atomic Aggregate -attribuutti on asetettu kyseiseen reittitietoon. Aggregator-attribuutti tarjoaa tiedon, missä reittitiedon yhdistäminen on tapahtunut. Aggregator-attribuutissa on sekä AS-numero että IP-osoite siitä reitittimestä, jossa reittitiedon yhdistäminen on tapahtunut.

Community-attribuutti

Community-attribuutilla voidaan merkitä reittitieto kuuluvaksi johonkin yhteisöön (comminity), jotka sisältävät yhden tai useamman yhteisen ominaisuuden. Palvelun-tarjoaja voi esimerkiksi liittää tietyille asiakasreiteille Comminity-attribuutin ja sen perusteella määrittää kyseisille reiteille Local Preference- ja Multiple Exit Discriminator -attribuutteja. Comminity-attribuutti on neljä tavuinen arvo, joka kuvataan usein merkinnällä AA:NN, jossa AA on autonomisen alueen numero ja NN on kyseistä yhteisöä kuvaava arvo.

7.4.4 Valintaiset Nontransitive-attribuutit

Multiple Exit Discriminator -attribuutti

Multiple Exit Discriminator -attribuutti (MED) lisätään reittimainoksiin eBGP-linkkiväleille ja se välitetään iBGP-osapuolille, mikä mahdollistaa vaikuttamisen autonomisen alueen ulospäin suuntautuvaan reititykseen. MED-attribuuttia ei välitetä toisiin autonomisiin alueisiin. MED-attribuutti on kuten perinteinen reititys arvo (metric), minkä perusteella osapuoli valitsee käytettävän reitin, kun edelliset päätöskohdat ovat olleet samoja. Mitä pienempi MED:n arvo on sitä parempi reitti on kyseessä. MED-attribuuttia käytetään siis mainostamaan naapuri autonomisille alueille mitä linkkiä pitkin olisi suositeltavaa lähettää liikennettä takaisin omaan autonomiseen alueeseen.

Originator ID -attribuutti

Originator ID -attribuuttia voidaan käyttää reittiheijastin reitittimissä. Attribuutilla pyritään estämään silmukoiden syntyminen. Originator ID -attribuutti on 32-bittinen arvo, jonka reittiheijastin luo. Arvo on reitittimen tunniste paikallisessa autonomisessa alueessa (yleensä reitittimen jokin loopback-osoite). Mikäli reittiheijastin havaitsee oman reitittimen tunnisteen reittimainoksen Originator ID -attribuutissa, se hylkää paketin, koska silmukka on syntynyt.

Cluster List -attribuutti

Cluster List -attribuutti on joukko reittiheijastin reitittimien ryhmätunnisteita, joiden kautta kyseinen reittitieto on kulkenut. Attribuutilla pyritään estämään silmukoiden syntyminen. Mikäli reittiheijastin reititin havaitsee oman paikallisen ryhmätunnisteen reittimainoksen Cluster List -attribuutissa, se hylkää paketin, koska silmukka on syntynyt.

7.4.5 BGP:n reititysvalinta

BGP-osapuoli suorittaa reititysvalintaprosessin valitakseen kahdesta tai useammasta reittitiedosta parhaan BGP-reitin kyseiseen kohteeseen. Kun paras reitti on valittu se lisätään reititystauluun. Eri reititinvalmistajat käyttävät hieman erilaista järjestystä/valintatapaa parhaimman reitin valitsemiseksi. Alla on esitetty kahden suurimman reititinvalmistajan valintaprosessi.

Cisco Systems:n IOS-käyttöjärjestelmän valintaprosessi (DeHaven Carroll & Doyle 2001, 115 - 116):

1. Suosi suurinta Weight-attribuutin omaavaa reittitietoa. Weigth-attribuutti on Ciscon oma attribuutti.
2. Jos Weight-attribuutin arvot ovat samat, suosi suurimman Local Preference -attribuutin omaavaa reittitietoa.
3. Jos Local Preference -attribuutin arvot ovat samat, suosi reittitietoa, joka on lähtöisin tästä reitittimestä.

4. Jos Local Preference -attribuutin arvot ovat samat ja reittitieto ei ole lähtöisen tästä reitittimestä, suosi lyhimmän AS Path -attribuutin omaavaa reittitietoa.
5. Jos AS-polun pituus on sama, suosi pienimmän Origin-koodin arvoa. IGP on pienempi kuin EGP, joka on edelleen pienempi kuin Unknown / Incomplete.
6. Jos Origin-koodit ovat samat, suosi pienimmän MED-arvon omaavaa reittitietoa.
7. Jos MED-arvot ovat samat, suosi eBGP reittejä ohi yhtymä (Confederation) eBGP-reittien. Yhtymä eBGP-reitit ovat edelleen suositeltavampia kuin iBGP-reitit.
8. Jos reitit ovat edelleen samat, suosi reittiä, jolla on lyhin polku Next Hop -attribuutin osoitteeseen.
9. Viimeisenä vaihtoehtona on suosia reittiä, jossa on pienin BGP-reitittimen tunniste.

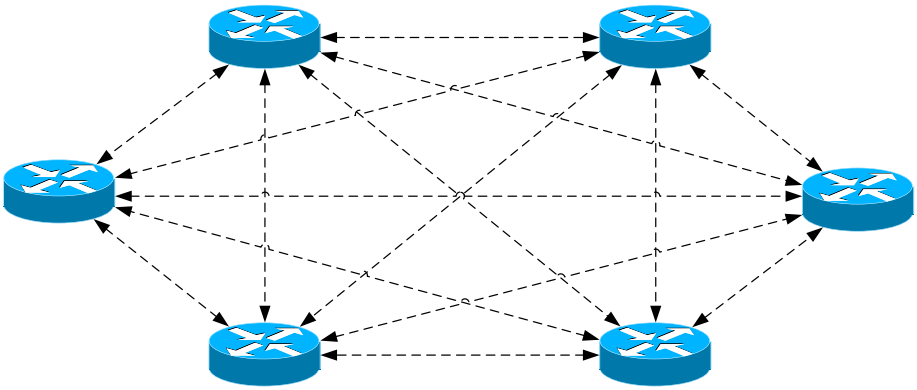
Juniper Networks:n JUNOS-käyttöjärjestelmän valintaprosessi (Marschke & Reynolds 2008, 205):

1. Voidaanko BGP:n Next Hop -attribuutin IP-osoite tavoittaa?
2. Suosi reittitietoa, jolla on korkein Local Preference -attribuutin arvo.
3. Suosi reittitietoa, jolla on lyhin AS Path -attribuutin pituus.
4. Suosi reittitietoa, jolla on pienin Origin-koodin arvo.
5. Suosi reittitietoa, jolla on pienin MED-arvo.
6. Suosi reittitietoa, joka on opittu eBGP:n kautta.
7. Suosi reittitietoa, jolla on alhaisin IGP-metriikan arvo:
    a. Tutki reititystauluista inet.0 ja inet.3 BGP:n Next Hop -attribuutissa oleva IP-osoite ja tämän jälkeen liitä se fyysinen seuraava hyppy reittiin, jossa on parempi preferenssi.
    b. Jos preferenssit ovat samat, liitä fyysinen seuraava hyppy, joka löytyy inet.3-taulusta.
    c. Jos preferenssit ovat samat saman reititystaulun sisällä, liitä fyysinen seuraava hyppy siihen mistä löytyy suurempi määrä samanarvoisia reittejä.
8. Suosi reittitietoa, jolla on lyhin ryhmän (Cluster) pituus.

9. Suosi reittitietoja, jotka tulevat pienimmän reitittittimentunnisteen omaavalta BGP-osapuolelta.
10. Suosi reittitietoja, jotka tulevat pienimmän osapuolen ID:n omaavalta reitittimeltä.

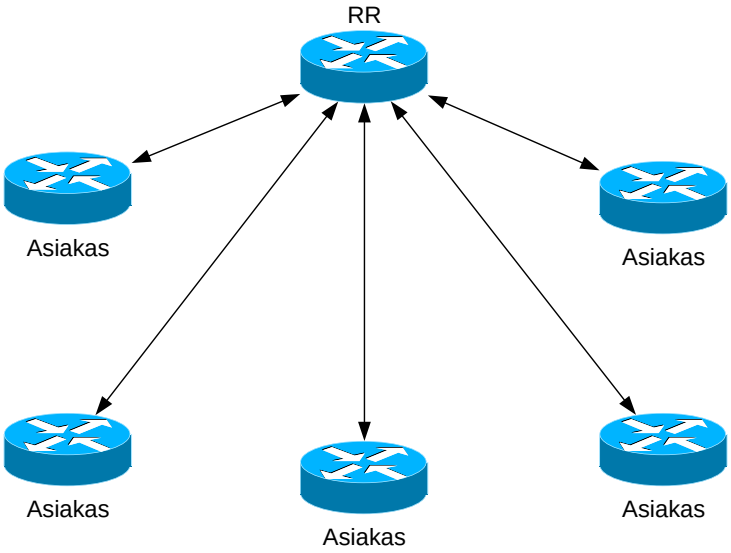
7.5 Reittiheijastin

Reittiheijastimia eli Route Reflector:ja (RR) käytetään vähentämään tarvetta luoda täysinkytkettyjä iBGP-istuntoja autonomisen alueen sisällä. Reittiheijastimet ovat käytännöllisiä, kun autonominen alue sisältää suuren määrän iBGP-osapuolia. Ellei eBGP:llä opittuja reittitietoja välitetä autonomisen alueen IGP-protollalle, tarvitsee kaikkien iBGP-osapuolien olla täysinkytkettyjä toisiinsa. Tästä aiheutuu suuri määrä iBGP-istuntoja. N-kappaletta reitittimiä kohti tulee n(n-1)/2 -kappaletta iBGP-istuntoja autonomisen alueen sisälle. Esimerkiksi kuuden täysinkytketyn iBGP-osapuolen verkossa tarvitaan 15 iBGP-istuntoa, kuten kuviossa 32 on nähtävissä.



KUVIO 32. Täysinkytketty iBGP-verkko

Käytettäessä reittiheijastimia yksi (tai useampi) reititin valitaan reittiheijastimeksi ja muut reitittimet ovat asiakasreitittimiä (client), jotka luovat ainoastaan iBGP-yhteyden reittiheijastimeen. Kuviosta 33 on nähtävissä kuuden reitittimen iBGP-verkko, jossa yksi reititin toimii reittiheijastimena.



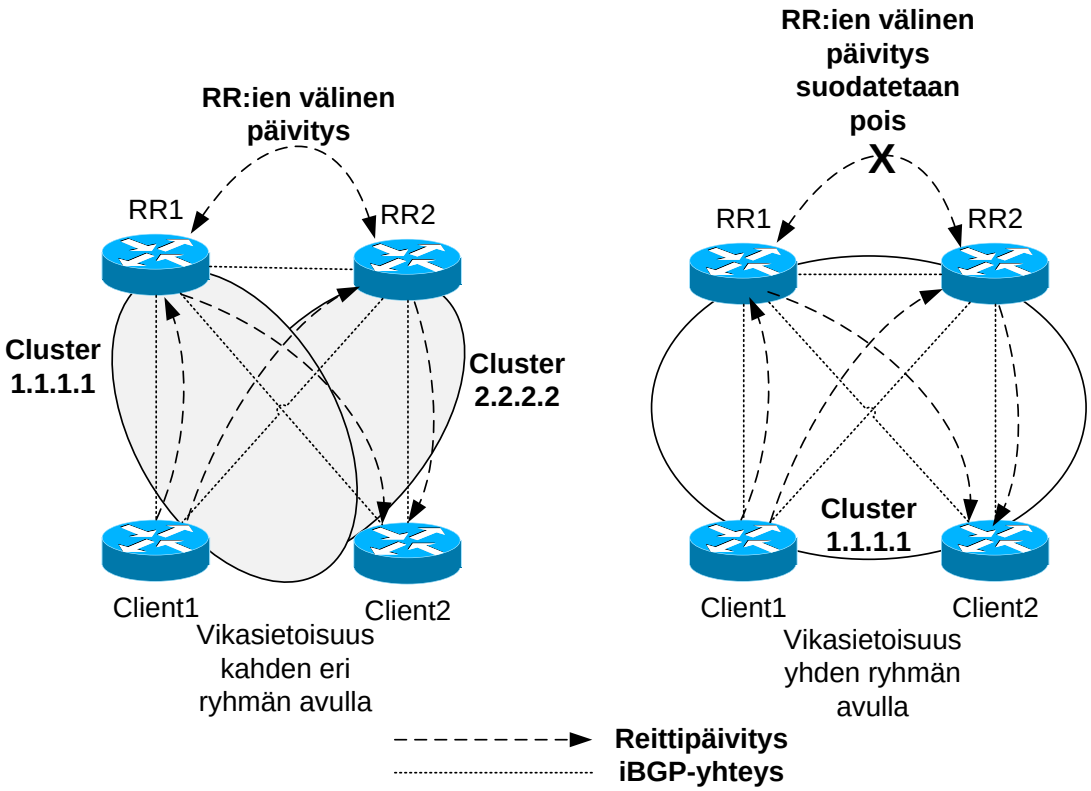
KUVIO 33. Reittiheijastinta käyttävä täysinkytketty iBGP-verkko

Vertaamalla kuvioissa 32 ja 33 näkyvien iBGP-yhteyksien määrää, voidaan helposti nähdä, että reittiheijastimet vähentävät radikaalisti iBGP-yhteyksien määrää jo suhteellisen pienessä verkossa. Tuloksena kuuden reitittimen kokoisessa verkossa yhteyksien määrä putosi 15 kappaleesta viiteen.

Reittiheijastimia käytettävät reitittimet estävät reittitietosilmukoiden syntymisen käyttämällä Originator ID- ja Cluster List -attribuutteja. Originator ID -attribuutti lisätään reittiheijastimen lähettämään reittipäivitykseen, jossa on sen reittitiedon lähteen BGP-tunniste. BGP-osapuolen ei tulisi luoda Originator ID -attribuuttia, jos sellainen on jo olemassa. BGP-osapuolen tulee hylätä sellainen reittitietopäivitys, jossa on Originator ID -attribuuttissa kyseisen BGP-osapuolen BGP-tunniste. Cluster List -attribuutti on joukko Cluster ID -arvoja, jotka kuvaavat reittitiedon kulkemien reittiheijastinryhmien tunnisteet. Kun reittiheijastin edelleenmainostaa reittiä, sen täytyy lisätä paikallinen Cluster ID -tunniste Cluster List -attribuuttiin. Käytettäessä Cluster List -attribuuttia reittiheijastin voi tarkistaa onko reittitieto kiertänyt takaisin samaan reittiheijastinryhmään konfiguraatiovirheen takia. Jos paikallinen Cluster ID -tunniste on reittitietopäivityksessä, se tulee hylätä. (Bates, Chandra & Chen 2006, 6.)

Pelkästään yhden reittiheijastimen käyttäminen verkossa ei ole järkevää, koska verkon toiminta riippuu yhdestä reitittimestä. Onkin järkevää luoda reittiheijastinryhmiä, joiden osapuolet muodostavat kaikkiin iBGP-verkon reitittimiin iBGP-yhteyden. On

olemassa kaksi eri ratkaisutapaa, miten lisätään vikasietoisuutta reittiheijastimia käytettäessä. Kuviossa 34 on vasemmalla puolella esitetty malli (tapa 1), jossa käytetään kahta erillistä reittiheijastinryhmää, ja oikealla on esitetty malli (tapa 2), jossa käytetään yhtä yhteistä reittiheijastinryhmää koko verkossa. (Marschke & Reynolds 2008, 211).



KUVIO 34. Reittiheijastimien vikasietoisuus (Marschke & Reynolds 2008, 211)

Tapa 1 mahdollistaa reittitietojen vaihtamisen myös reittiheijastimien välillä, koska reittiheijastin ei näe reittimainostuksessa omaa reittiheijastinryhmän tunnusta (Cluster ID). Tämä mahdollistaa, että reittiheijastimet oppivat myös sekä reittiheijastinryhmän sisäisiä reittietoja että reittiheijastinryhmien välisiä reittitietoja, mikä johtaa täydellisempään BGP-reittitauluun. Esimerkiksi jos yhteys RR1-reitittimen ja Client1-reitittimen välillä katkeaa ja menetään iBGP-yhteys, on RR1-reitittimellä silti mahdollisuus tavoittaa Client1-reititin, koska reittitieto on opittu myös RR2-reitittimen kautta käyttäen reittiheijastinryhmää 2.2.2.2. Kahden tai useamman reittiheijastinryhmän

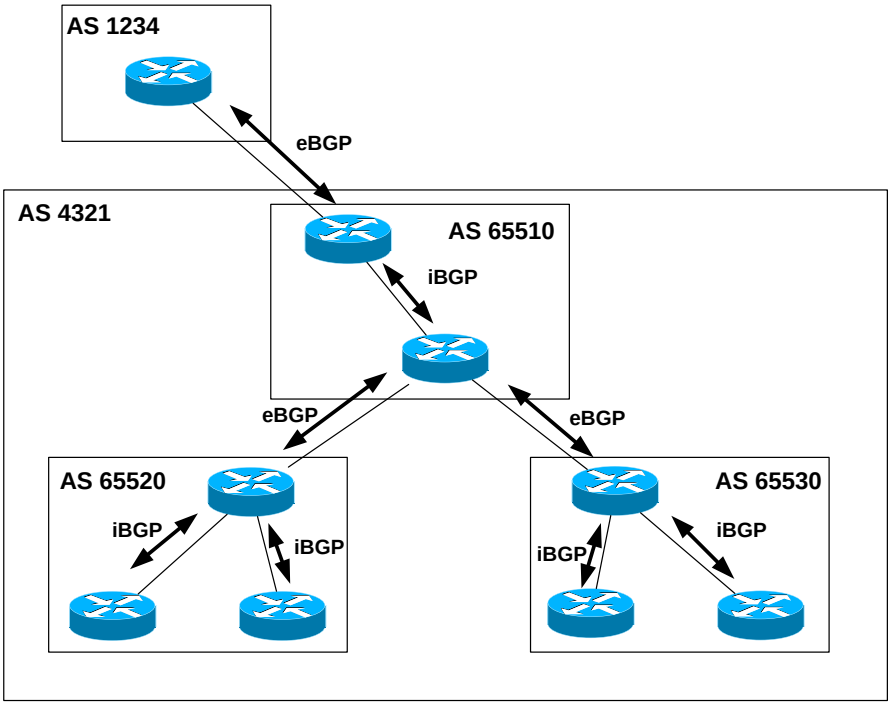
käyttäminen lisää BGP-reittitaulujen kokoa reittiheijastinreitittimissä. (Marschke & Reynolds 2008, 211).

Tavassa 2 reittiheijastinreitittimet eivät välitä toisilleen reittitietoja, koska reittipäivitysviestit sisältävät saman Cluster ID:n, jolloin reititin hylkää reittipäivitysviestin. (Marschke & Reynolds 2008, 211).

Käytettäessä Loopback-rajapintoja hyödyntäviä iBGP-yhteyksiä, on olemassa hyvin pieni riski siihen, että Client:n ja reittiheijastimen välinen yhteys katkeaisi ja Client pystyisi samanaikaisesti ylläpitämään muut BGP-yhteydet verkossa. Tästä syystä kahden tai useamman reittiheijastinryhmän käyttäminen on suositeltavaa ainoastaan, jos käytössä on fyysisiin rajapintoihin sidotut iBGP-yhteydet. (Marschke & Reynolds 2008, 211).

7.6 BGP-konfederaatio

BGP-konfederaatio jakaa tehokkaasti yhden suuren autonomisen alueen useaan pienempään autonomiseen alueeseen. Yhden konfederaation sisällä voidaan luoda täysinkytketty iBGP-verkko tai käyttää reittiheijastimia alueen sisäisiin reittietojen vaihtamisiin ja eBGP-yhteyttä reittitietojen välitykseen muihin konfederaatioihin tai autonomisiin alueisiin. Kuviossa 35 on esitetty esimerkki, miten BGP-konfederaatioita voidaan käyttää vähentämään iBGP-yhteyksien määrää. (DeHaven Carroll & Doyle 2001, 131 - 132).



KUVIO 35. Esimerkki BGP-konfederaatioista

Kuviossa 35 on nähtävissä miten autonominen alue 4321 on jaettu kolmeen konfederaatioon, joiden välillä käytetään eBGP-yhteyttä välittämään reittitietoja ja konfederaatioiden sisällä reittitietoja välitetään käyttäen iBGP:aa.

8 KÄYTÄNNÖN TOTEUTUS

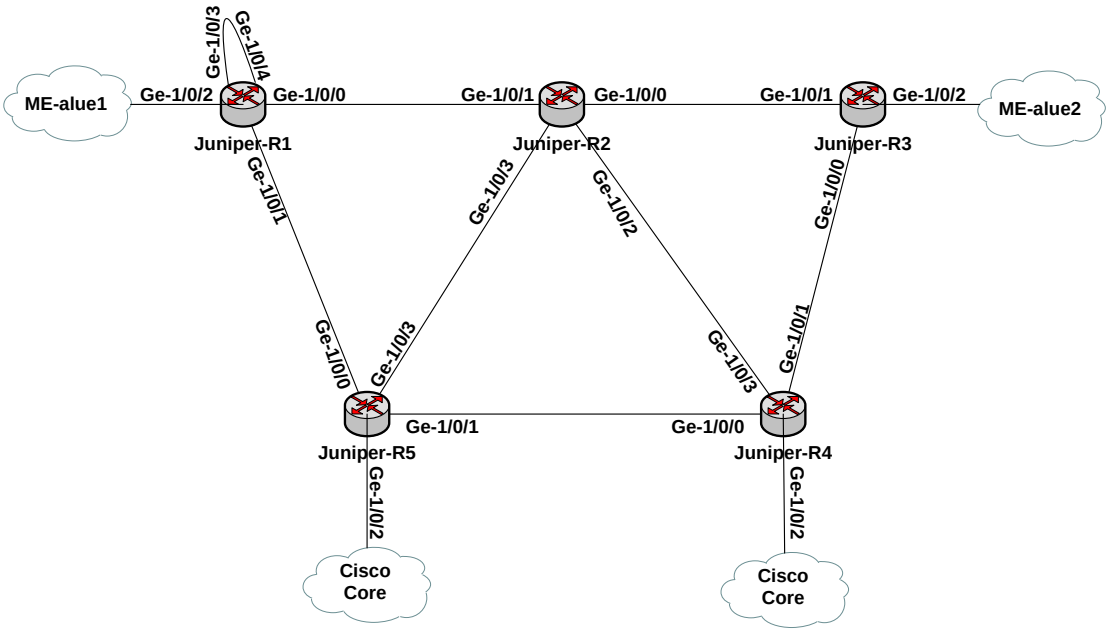
8.1 Topologiat, laitteistot ja IP-osoitteet

8.1.1 Operaattori

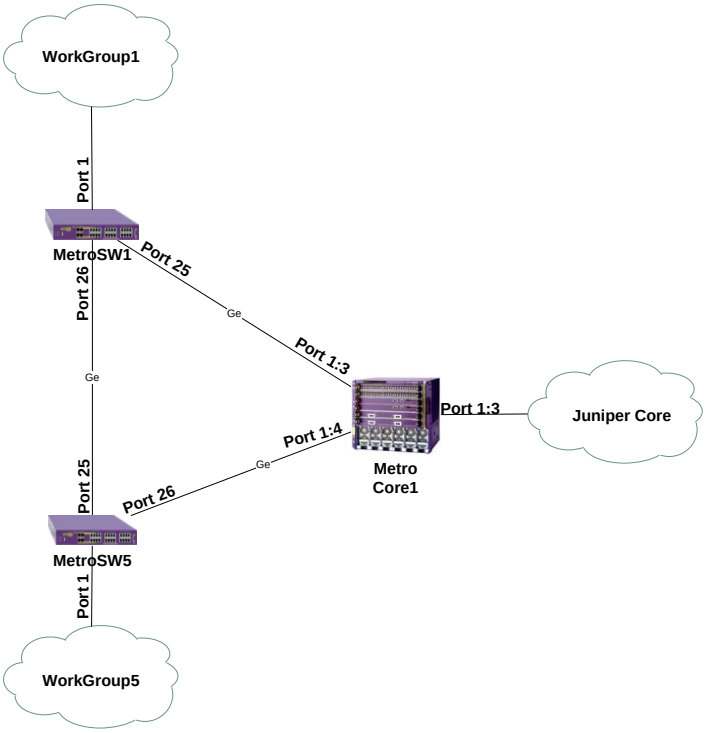
Operaattoriverkoksi valitsin SpiderNet:n laitteista Juniper Core- ja Metro Core -laitteet, koska näiden avulla oli mahdollista toteuttaa yleisesti käytettävissä olevien operaattoriverkkojen kaltainen ympäristö. Operaattoriverkon vaatimuksina oli työntavoitteissa määritetty: MPLS-runkoverkko, Metro Ethernet -alueet ja tuki VPLS-tekniikalle. Juniper Core -laitteet soveltuivat parhaiten toteutettavaan runkoverkkoon, koska niiden avulla oli mahdollista toteuttaa verkkoon myös VPLS-toiminteita. Metro Core oli luonnollinen valinta Metro Ethernet -alueiden luomiseen, koska Metro Core -

laitteet tukevat kaikkia tarvittavia protokollia ja tekniikoita Metro Ethernet -alueen luomiseen.

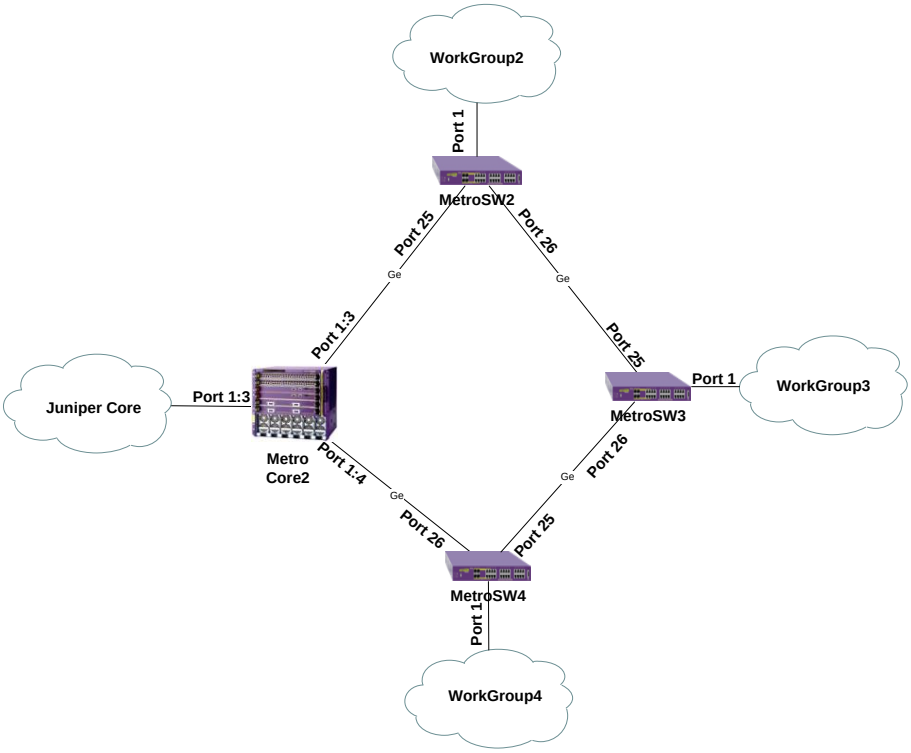
Operaattorin verkkotopologia koostuu siis SpiderNet:n eri verkkotopologioista. Metro Ethernet -alueisiin käytetään kahta Metro Core:n rengasta. Renkaat ovat kytkettyinä eri puolille Juniper Core:a, kuten kuvioista 36, 37 ja 38 on nähtävissä.



KUVIO 36. Operaattorin runkoverkko



KUVIO 37. Metro Ethernet -alue 1



KUVIO 38. Metro Ethernet -alue 2

Kuviosta 36 nähdään, että Juniper Core eli operaattorin runkoverkko muodostuu viidestä J-series J2320-reitittimestä. Työnteko hetkellä reitittimissä oli JUNOS-käyttöjärjestelmän versio 9.5. Reitittimien välillä on kytkennät tehty mesh-tyyppisesti eli verkossa on useita eri reittivaihtoehtoja eri reitittimien välille. Taulukossa 7 on esitetty runkoverkon eli Juniper Core:n fyysinen kaapelointi.

TAULUKKO 7. Juniper Core:n fyysinen kaapelointi

Lähdelaite	**Lähdeportti**	**Kohdelaite**	**Kohdeportti**
Juniper-R1	Ge-1/0/0	Juniper-R2	Ge-1/0/1
Juniper-R1	Ge-1/0/1	Juniper-R5	Ge-1/0/0
Juniper-R1	Ge-1/0/2	MetroCore1	Port 1:5
Juniper-R1	Ge-1/0/3	Juniper-R1	Ge-1/0/4
Juniper-R2	Ge-1/0/0	Juniper-R3	Ge-1/0/1
Juniper-R2	Ge-1/0/1	Juniper-R1	Ge-1/0/0
Juniper-R2	Ge-1/0/2	Juniper-R4	Ge-1/0/3
Juniper-R2	Ge-1/0/3	Juniper-R5	Ge-1/0/3
Juniper-R3	Ge-1/0/0	Juniper-R4	Ge-1/0/1
Juniper-R3	Ge-1/0/1	Juniper-R2	Ge-1/0/0
Juniper-R3	Ge-1/0/2	MetroCore2	Port 1:5
Juniper-R4	Ge-1/0/0	Juniper-R5	Ge-1/0/1
Juniper-R4	Ge-1/0/1	Juniper-R3	Ge-1/0/0
Juniper-R4	Ge-1/0/2	CiscoCore-R3	Fe 3/2
Juniper-R4	Ge-1/0/3	Juniper-R2	Ge-1/0/2
Juniper-R5	Ge-1/0/0	Juniper-R1	Ge-1/0/1
Juniper-R5	Ge-1/0/1	Juniper-R4	Ge-1/0/0
Juniper-R5	Ge-1/0/2	CiscoCore-R1	Fe 3/3
Juniper-R5	Ge-1/0/3	Juniper-R2	Ge-1/0/3

Taulukossa 8 on esitetty runkoverkon linkkivälien IP-osoitteet.

TAULUKKO 8. Runkoverkon IP-osoitteet

Lähtöpää	**Portti**	**IP-osoite**	**Kohdepää**	**Portti**	**IP-osoite**
Juniper-R1	Ge-1/0/0	10.0.0.1/24	Juniper-R2	Ge-1/0/1	10.0.0.2/24
Juniper-R1	Ge-1/0/4.101	130.100.8.1/30	-	-	-
Juniper-R2	Ge-1/0/0	10.0.1.1/24	Juniper-R3	Ge-1/0/1	10.0.1.2/24
Juniper-R3	Ge-1/0/0	10.0.2.1/24	Juniper-R3	Ge-1/0/1	10.0.2.2/24
Juniper-R4	Ge-1/0/0	10.0.3.1/24	Juniper-R4	Ge-1/0/1	10.0.3.2/24
Juniper-R5	Ge-1/0/0	10.0.4.1/24	Juniper-R1	Ge-1/0/1	10.0.4.2/24
Juniper-R2	Ge-1/0/3	10.0.5.1/24	Juniper-R5	Ge-1/0/3	10.0.5.2/24
Juniper-R2	Ge-1/0/2	10.0.6.1/24	Juniper-R4	Ge-1/0/3	10.0.6.2/24
Juniper-R4	Ge-1/0/2	210.10.1.1/30	CiscoCore-R3	Fe 3/2	210.10.1.2/30
Juniper-R5	Ge-1/0/2	210.10.1.5/30	CiscoCore-R1	Fe 3/3	210.10.1.6/30

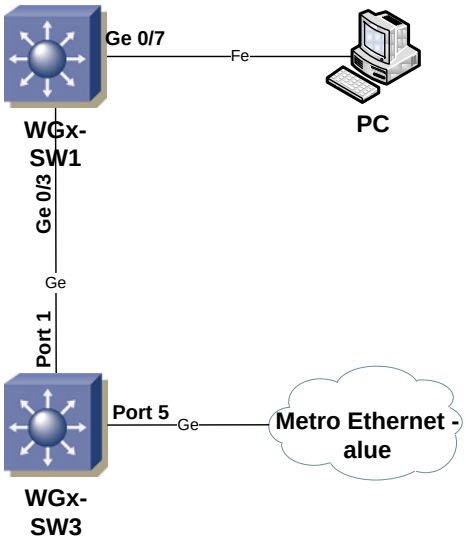
Viiden reitittimen muodostama kokonaisuus mahdollistaa kahden PE-laitteen toteuttamisen runkoverkkoon. PE-laite on kytketty MetroCore1- tai MetroCore2-laitteeseen riippuen siitä kumman puolen PE-laitteesta on kyse. MetroCoreX-laite on puolestaan kytketty kahteen MetroSWx-kytkimeen, mistä muodostuu rengastopologia kumpaankin Metro Ethernet -alueeseen. Jokaisesta MetroSWx-kytkimestä on yhteys vastaavan WorkGroup:n L3-kytkimeen. Taulukossa 9 on esitetty fyysinen kaapelointi operaattorin Metro Ethernet -alueissa. Järkevin vaihtoehto olisi ollut toteuttaa suoraan rengastopologia PE-laitteesta liityntäverkkoon, mutta SpiderNet:n topologia ei tätä mahdollistanut.

TAULUKKO 9. Metro Ethernet -alueiden fyysinen kaapelointi

Lähdelaite	Lähdeportti	Kohdelaite	Kohdeportti
MetroCore1	Port 1:3	MetroSW1	Port 25
MetroCore1	Port 1:4	MetroSW5	Port 26
MetroCore1	Port 1:5	Juniper-R1	Ge-1/0/2
MetroCore2	Port 1:3	MetroSW2	Port 25
MetroCore2	Port 1:4	MetroSW4	Port 26
MetroCore2	Port 1:5	Juniper-R3	Ge-1/0/2
MetroSW1	Port 1	WG1-SW3	Port 5
MetroSW1	Port 25	MetroCore1	Port 1:3
MetroSW1	Port 26	MetroSW5	Port 26
MetroSW2	Port 1	WG2-SW3	Port 5
MetroSW2	Port 25	MetroCore2	Port 1:3
MetroSW2	Port 26	MetroSW3	Port 26
MetroSW3	Port 1	WG3-SW3	Port 5
MetroSW3	Port 25	MetroSW2	Port 26
MetroSW3	Port 26	MetroSW4	Port 25
MetroSW4	Port 1	WG4-SW3	Port 5
MetroSW4	Port 25	MetroSW3	Port 26
MetroSW4	Port 26	MetroCore2	Port 1:4
MetroSW5	Port 1	WG5-SW3	Port 5
MetroSW5	Port 25	MetroSW1	Port 26
MetroSW5	Port 26	MetroCore1	Port 1:4

8.1.2 WorkGroup

Tässä työssä WorkGroup:t yksi ja kaksi kuvaavat yrityksen Yritys1 kahta toimipistettä, jotka sijaitsevat eri puolilla Operaattorin runkoverkkoa. WorkGroup:ien L3-kytkin hoitaa asiakasverkon reitityksen ja liittää asiakkaan Operaattorin liityntäverkkoon Ethernet-yhteydellä, johon lähetetään paketit asiakkaan VLAN-tiedoilla merkattuina (ks. kuvio 39). Johtuen SpiderNet:n topologiasta, asiakasverkon (WorkGroup:n) ja Operaattorin liityntäverkon välillä on yksi kytkin, joka käytännössä ainoastaan välittää VLAN-leimattuja kehyksiä eteenpäin eli se ei vaikuta verkon toimintaan mitenkään.



KUVIO 39. WorkGroup-topologia

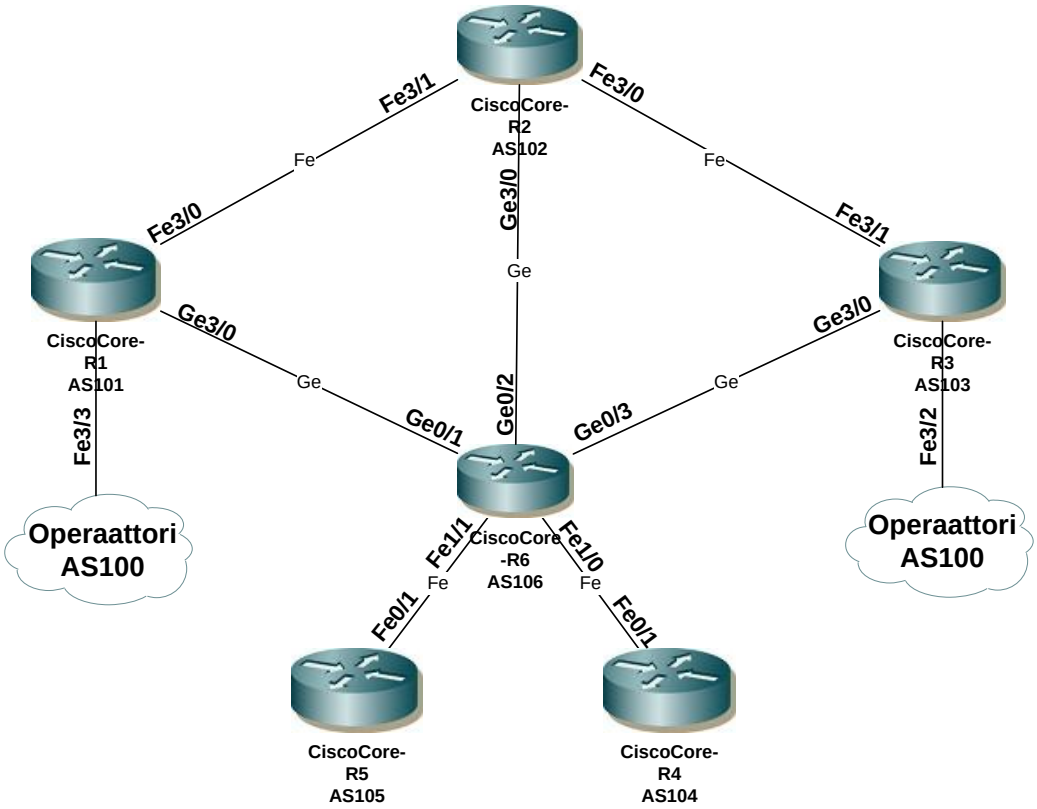
Taulukossa 10 on esitetty Yritys1:n käyttämät IP-osoitteet.

TAULUKKO 10. Yritys1:n käyttämät IP-osoitteet

Laite	**Rajapinta**	**IP-osoite**	**Selite**
WG1-SW1	VLAN 10	192.168.10.1/24	VLAN 10 -rajapinta
WG1-SW1	VLAN 20	192.168.20.1/24	VLAN 20 -rajapinta
WG1-SW1	VLAN 130	130.100.10.1/24	Julkisen verkon reititysrajapinta
WG1-SW1	VLAN 1001	130.100.8.2/30	Reititysrajapinta
PC 1	Verkkosovitin	192.168.10.10/24	Työasema WorkGroup1:n VLAN 10:ssä
PC 2	Verkkosovitin	192.168.10.20/24	Työasema WorkGroup2:n VLAN 10:ssä
WG2-SW1	VLAN 10	192.168.10.2/24	VLAN 10 -rajapinta
WG2-SW1	VLAN 20	192.168.20.2/24	VLAN 20 -rajapinta

8.1.3 “Internet”

Internet on tässä työssä toteutettu Cisco Core -laitteilla, joista jokainen reititin muodostaa oman autonomisen alueen. Reitittimien Loopback-rajapinnat vastaavat kyseisen operaattorin mainostamia verkkoja. Kuviossa 40 on esitetty käytettävä Cisco Core -topologia, josta näkyy myös liitynnät Operaattorin verkkoon.



KUVIO 40. "Internet"-topologia

Internetiä simuloivien verkkojen ja linkkivälien IP-osoitteet on nähtävissä taulukossa 11.

TAULUKKO 11. "Internetin" IP-osoitteet

Lähtöpää	**Portti**	**IP-osoite**	**Kohdepää**	**Portti**	**IP-osoite**
CiscoCore-R1	Fe 3/3	210.10.1.6/30	Juniper-R5	Ge-1/0/2	210.10.1.5/30
CiscoCore-R1	Ge3/0	210.10.1.9/30	CiscoCore-R6	Ge0/1	210.10.1.10/30
CiscoCore-R1	Fe 3/0	210.10.1.13/30	CiscoCore-R2	Fe 3/1	210.10.1.14/30
CiscoCore-R1	Loopback 1	80.0.0.1/17			
CiscoCore-R1	Loopback 2	85.0.128.1/19			
CiscoCore-R2	Fe 3/1	210.10.1.14/30	CiscoCore-R1	Fe 3/0	210.10.1.13/30
CiscoCore-R2	Fe 3/0	210.10.1.17/30	CiscoCore-R3	Fe 3/1	210.10.1.18/30
CiscoCore-R2	Ge 3/0	210.10.1.21/30	CiscoCore-R6	Ge 0/2	210.10.1.22/30
CiscoCore-R2	Loopback 1	12.0.0.1/8			
CiscoCore-R3	Fe 3/2	210.10.1.2/30	Juniper-R4	Ge-1/0/2	210.10.1.1/30
CiscoCore-R3	Ge 3/0	210.10.1.25/30	CiscoCore-R6	Ge 0/3	210.10.1.26/30
CiscoCore-R3	Fe 3/1	210.10.1.16/30	CiscoCore-R2	Fe 3/0	210.10.1.17/30
CiscoCore-R3	Loopback 1	200.30.0.1/19			
CiscoCore-R3	Loopback 2	200.35.0.1/21			
CiscoCore-R4	Ge 3/0	210.10.1.29/30	CiscoCore-R4	Ge 3/0	210.10.1.30/30
CiscoCore-R4	Fe 0/1	210.10.1.33/30	CiscoCore-R6	Fe 1/0	210.10.1.34/30
CiscoCore-R4	Loopback 1	100.80.192.1/18			
CiscoCore-R5	Ge 3/0	210.10.1.30/30	CiscoCore-R4	Ge 3/0	210.10.1.29/30
CiscoCore-R5	Fe 0/1	210.10.1.37/30	CiscoCore-R6	Fe 1/1	210.10.1.38/30
CiscoCore-R5	Loopback 1	30.10.0.1/16			
CiscoCore-R5	Loopback 2	191.145.224.1/1			
CiscoCore-R6	Ge 0/1	210.10.1.10/30	CiscoCore-R1	Ge 3/0	210.10.1.9/30
CiscoCore-R6	Ge 0/2	210.10.1.22/30	CiscoCore-R2	Ge 3/0	210.10.1.21/30
CiscoCore-R6	Ge 0/3	210.10.1.26/30	CiscoCore-R3	Ge 3/0	210.10.1.25/30
CiscoCore-R6	Fe 1/0	210.10.1.34/30	CiscoCore-R4	Fe 0/1	210.10.1.33/30
CiscoCore-R6	Fe 1/1	210.10.1.38/30	CiscoCore-R5	Fe 0/1	210.10.1.37/30
CiscoCore-R6	Loopback 1	150.40.64.1/18			
CiscoCore-R6	Loopback 2	196.197.208.1/2			

8.2 Operaattorin runkoverkon konfigurointi

8.2.1 OSPF-konfigurointi

Operaattorin runkoverkon konfiguroinnin aloitin IGP-reititysprotokollan konfiguroinnilla. Valitsin IGP-reititysprotokollaksi OSPF:n, koska kyseinen protokolla on itselleni kaikkein tutuin IGP-reititysprotokollista ja yleisimmin käytetty reititysprotokolla operaattorien runkoverkoissa. OSPF:n konfigurointi JUNOS:ssa on varsin helppoa ja yksinkertaista. Kun OSPF-alueen rajapinnoissa on määritetty IP-osoitteet, riittää, että kyseiset rajapinnat lisätään OSPF-protokollaan. Konfigurointivaihtoehtona on joko siirtyä oikeaan hierarkiatasoon tai antaa suora *set*-komento ylimmältä hierarkiatasolta. Esimerkkinä Juniper-R1:n OSPF-konfigurointi siirtymällä oikeaan hierarkiatasoon:

root@Juniper-R1# edit protocols ospf area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
root@Juniper-R1# set interface ge-1/0/0.0
root@Juniper-R1# set interface ge-1/0/1.0

Tai vaihtoehtoisesti OSPF-konfigurointi suoraan ylimmältä hierarkiatasolta:

root@Juniper-R1#set protocols ospf area 0.0.0.0 interface ge-1/0/0.0
root@Juniper-R1#set protocols ospf area 0.0.0.0 interface ge-1/0/1.0

OSPF-reititykseen on hyvä lisätä myös Loopback-rajapinta, koska oletuksena JUNOS käyttää Loopback-rajapinnan osoitetta Router-ID:nä:

root@Juniper-R1#set protocols ospf area 0.0.0.0 interface loopback 0.0

8.2.2 LDP- ja MPLS-konfigurointi

LDP- ja MPLS-protokollien konfigurointi on lähes yhtä yksinkertaista kuin OSPF:n. Kummankin protokollan määrityksiin lisätään ne rajapinnat, jotka osallistuvat LDP-viestien vaihtoon ja MPLS-verkkoon. MPLS-alueeseen kuuluville rajapinnoille täytyy ensimmäisenä kertoa, että ne kuuluvat ”MPLS-perheeseen”, jonka jälkeen voidaan

kyseiset rajapinnat konfiguroida LDP- ja MPLS-protokolliin. Esimerkkinä Juniper-R1:n LDP:n ja MPLS:n konfigurointi:

root@Juniper-R1# set interface ge-1/0/0 unit 0 family mpls
root@Juniper-R1# edit protocols mpls
[edit protocols mpls]
root@Juniper-R1# set interface ge-1/0/0.0
root@Juniper-R1# set interface ge-1/0/1.0

root@Juniper-R1# edit protocols ldp
[edit protocols ldp]
root@Juniper-R1# set interface ge-1/0/0.0
root@Juniper-R1# set interface ge-1/0/1.0

Lisäksi tarvitsee määrittää Security-hierarkian alle MPLS:n yhteydessä käytettävä pakettipohjainen liikenteenvälitystapa:

root@Juniper-R1# edit security forwarding-options family mpls
[edit security forwarding-options family mpls]
root@Juniper-R1# set mode packet-based

Juniper-laitteiden kokonaiset konfiguraatiot ovat liitteissä 3 - 9.

8.3 Metro Ethernet -alueiden konfigurointi

8.3.1 EAPS:n konfigurointi

Metro Ethernet -alueisiin tarvitsi konfiguroida silmukanestomenetelmä, jona tässä työssä käytin EAPS:ia johtuen käytettävästä laitevalmistajasta. EAPS:n konfigurointi vaatii, että silmukkaan konfiguroidaan yksi isäntäsolmu ja sille ensisijainen- ja toissijainenportti. Muut EAPS-alueen solmut konfiguroidaan välityssolmuiksi. Alla on esimerkkinä MetroCore1:n EAPS-konfigurointi:

create eaps ME_area1
configure eaps ME_area1 mode master
configure eaps ME_area1 primary port 1:3
configure eaps ME_area1 secondary port 1:4

Lisäksi EAPS-aluetta varten tarvitsi luoda hallinta-VLAN, jota pitkin EAPS:n hallintaviestit kulkevat, ja joukko suojattuja VLAN:ja, joissa kuljetaan asiakasliikennettä. Asiakas-VLAN:t ja hallinta-VLAN:t ovat Metro Ethernet:n tapauksessa 802.1ad-VMAN:ja, jotka liitetään EAPS:iin. Alla esimerkkinä hallinta-VMAN:n luonti MetroCore1:een ja sen liittäminen EAPS-alueen hallinta-VLAN:ksi:

create vman ME_area1_control
configure vman ME_area1_control tag 101
configure vman ME_area1_control add ports 1:3,1:4 tagged
configure eaps ME_area1 add control vlan ME_area1_control

8.3.2 802.1ad:n eli QinQ:n konfigurointi

Metro Ethernet -alueisiin konfiguroitiin myös asiakas-VMAN:t, kullekin asiakkaalle omansa. QinQ:n konfigurointi on suoraviivainen toimenpide, ensin luodaan haluttu VMAN ja määritellään sille tunnisteen arvo, minkä jälkeen se tarvitsee lisätä EAPS-renkaan portteihin leimattuna ja yritykselle menevään porttiin ei-leimattuna. Lisäksi tarvitsee luotu VMAN liittää EAPS:ssa suojeltavaksi VLAN:ksi. Esimerkkinä on MetroSW1:lle Yritys1-VMAN:n konfigurointi, johon myös Yritys1:n WG1-SW3-kytkin on liitetty porttiin 1:

create vman yritys1
configure vman yritys1 tag 512
configure vman yritys1 add ports 25,26 tagged
configure vman yritys1 add ports 1 untagged
configure eaps ME_area1 add protected vlan yritys1

Jouduin käyttämään yrityksien leima-arvoina 512 tai suurempia arvoja, koska Juniperin J-Series vaatii leiman käsittelyssä kyseisiä arvoja.

Lisäksi tarvitsi muuttaa VMAN:n Ethertype-arvoa, koska Juniper:n J-Series tukee ainoastaan 0x8100, 0x9100 ja 0x9901 Ethertype:jä:

configure vman ethertype 0x8100

Metro Ethernet -alueiden kokonaiset konfiguraatiot löytyvät liitteistä 10 - 16.

8.4 VPLS-tekniikan konfigurointi

8.4.1 VPLS BGP-signaloinnilla

Juniper:n reitittimissä VPLS:n toteuttamiseen tarvitsi tehdä konfiguraatioita rajapintoihin, BGP-protokollaan sekä luoda reititysinstanssi VPLS:lle.

Juniper-R1:n MetroCore1:een liitettyyn rajapintaan ge-1/0/2 täytyi luoda looginen rajapinta kullekin asiakkaalle, jossa liikenteet erotellaan 802.1q-standardin mukaisella leimalla. Eli käytännössä Juniper-R1 tarkistaa vain uloimman leiman, vaikka MetroCore1:n lähettääkin kaikki kehykset 802.1ad-leimattuina. Käytettäessä *vlan-tagging*-leimausta, Juniper J-Series reitittimet tukevat ainoastaan VLAN-tunnisteita 512 - 4096 Gigabit Ethernet -rajapinnoille. Lisäksi tarvitsi määrittää VPLS-kapselointitapa rajapintaan ja käytettävä rajapintaperhe. Valitsin käytettäväksi kapseloinitavaksi Extended-vlan-vpls:n, koska siinä on tuettuna muitakin Ethertype-arvoja (0x8100, 0x9100 ja 0x9901) kuin pelkästään standardin mukainen 0x8100. Tämän jälkee loin loogisen rajapinnan Yritys1:lle sekä määritin, että kyseinen asiakkuus tunnistetaan VLAN-ID:n arvolla 512, ja määritin loogisen rajapinnan perheeksi VPLS:n. Esimerkkinä on Juniper-R1:n rajapinnan ge-1/0/2 VPLS-konfigurointi:

root@Juniper-R1# edit interface ge-1/0/2
[edit interface ge-1/0/2]
root@Juniper-R1# set vlan-tagging
root@Juniper-R1# set extended-vlan-vpls
root@Juniper-R1# set unit 101 vlan-id 512
root@Juniper-R1# set unit 101 family vpls

Alkuperäisen suunnitelmani mukaan tarkoitus oli käyttää stacked-vlan-tagging-ominaisuutta, jossa käytettäisiin pinottujen VLAN:ien tunnistamista eli QinQ:ta asiakkaiden erotteluun, mutta pitkällisten selvittelyjen jälkeen sain selville laitetoimittaja Cygate Oy:ltä, että kyseisen ominaisuuden näkyminen J-Series-laitteissa on todennäköisesti ohjelmistovirhe. Kyseinen toiminnallisuus ei siis ollut käytettävissä vaan oli tarve kehittää uusi ratkaisu miten VPLS-asiakkuus saadaan myös reititykseen ja sitä kautta luotua asiakkaalle ”Internet”-yhteys.

Ratkaisun ideoinnissa tarvittiin ulkopuolista apua, jota antoi Juniper Networks Certified Internet Expert (JNCIE) Antti Järvenpää Cygate Oy:stä. Hän kehitti ratkaisun, jossa lisättiin Juniper-R1:een lenkkikaapeli kahden rajapinnan väliin. Lenkkikaapelin toinen pää (ge-1/0/3) liitettäisiin asiakkaan VPLS-instanssin ja rajapinnassa kehyksestä poistettaisiin ulompi VLAN-leima, minkä jälkeen lenkkikaapelin jälkimmäinen pää (ge-1/0/4) erottelisi asiakkaan liikenteen asiakas-VLAN:n perusteella reititykseen. Alla on molempien rajapintojen konfiguraatiot:

root@Juniper-R1# edit interface ge-1/0/3
[edit interface ge-1/0/3]
root@Juniper-R1# set vlan-tagging
root@Juniper-R1# set extended-vlan-vpls
root@Juniper-R1# edit unit 101
[edit interface ge-1/0/3 unit 101]
root@Juniper-R1# set vlan-id 1001
root@Juniper-R1# set family vpls
root@Juniper-R1# set input-vlan-map push vlan-id 512
root@Juniper-R1# set output-vlan-map pop
root@Juniper-R1#top edit interface ge-1/0/4
[edit interface ge-1/0/4]
root@Juniper-R1# set vlan-tagging
root@Juniper-R1# set unit 101 vlan-id 1001
root@Juniper-R1# set unit 101 family inet address 130.100.8.1/30

Ylläolevissa konfiguraatioissa rajapinta ge-1/0/3 asetettiin käyttämään VLAN-leimausta sekä kapselointia *extended-vlan-vpls.* Tämän jälkeen luotiin looginen rajapinta eli asiakasrajapinta *unit 101*, johon määritettiin käytettävä VLAN-ID 1001, joka on siis asiakkaan käyttämä VLAN-tunniste julkiselle liikenteelle. Asiakas lähettää kaiken omasta verkosta ulos lähtevän liikenteen VLAN-ID:llä 1001. Loogisessa rajapinnassa tulevalle liikenteelle lisätään komenolla *set input-vlan-map push vlan-id 512* VLAN-leima tunnisteella 512, joka on siis Yritys1:lle määritetty VMAN-tunniste Metro Ethernet -alueissa. Rajapinnasta lähtevästä liikenteestä poistetaan ulompi leima komennolla *set output-vlan-map pop*, mikä mahdollistaa lenkkikaapelin ge-1/0/4-rajapinnassa liikenteen erottelun loogisessa rajapinnassa VLAN-ID:n 1001 perusteella. Ge-1/0/4-rajanpinnan loogiselle rajapinnalle annetaan asiakkaan välisen IP-osoiteparin toinen julkinen IP-osoite.

Lenkkikaapelin käyttäminen on mahdollista, koska samaan VPLS-instanssiin kuuluvat rajapinnat ovat kytkettynä toisiinsa automaattisesti.

Seuraavaksi tuli luoda VPLS-instanssi Yritys1:lle. Tämä tehtiin lisäämällä uusi reititysinstanssi, jonka nimenä käytin Yritys1_VPLS:

root@Juniper-R1# edit routing-instance Yritys1_VPLS
[edit routing-instance Yritys1_VPLS]
root@Juniper-R1# set instance-type vpls
root@Juniper-R1# set interface ge-1/0/2.101
root@Juniper-R1# set interface ge-1/0/3.101
root@Juniper-R1# set route-distinguisher 100:101
root@Juniper-R1# set vrf-target target:100:101
root@Juniper-R1# edit protocols vpls
[edit routing-instance Yritys1_VPLS protocols vpls]
root@Juniper-R1# set site-range 20
root@Juniper-R1# set no-tunnel-services
root@Juniper-R1# edit site Yritys1_WG1
[edit routing-instance Yritys1_VPLS protocols vpls site Yritys1_WG1]
root@Juniper-R1# set site-identifier 1
root@Juniper-R1# set interface ge-1/0/2.101 interface-mac-limit 20000

Ylläolevissa konfiguraatioissa määritettiin yhden VPLS-instanssin tarvitsemat konfiguraatiot. Ensimmäisenä luotiin VPLS-instanssi ja määritettiin sille instanssin tyypiksi VPLS sekä lisättiin instanssiin kuuluvat loogiset rajapinnat. Juniper-R1:lle tarvitsi lisätä kaksi rajapintaa, koska Yritys1:n liittäminen reititykseen tapahtui Juniper-R1:llä. Tämän jälkeen määritettiin käytettävä Route-Distinguisher-attribuutti, joilla erotellaan eri VPLS-instanssit, ja VRF-Target -attribuutti, jolla määritetään mistä RD-ryhmistä tuodaan reittejä tai mihin RD-ryhmään viedään reittejä. Seuraavaksi tuli määritellä VPLS-protokollan ominaisuuksia. Komennolla *set site-range* määritettiin kuinka monta Site:ä eli toimipistettä voi VPLS-instanssissa olla. Tällä määritetään siis kuinka monta eri *site-identifier*:ia kyseiseen VPLS-instanssiin voi kuulua. VPLS oletuksena vaatii Tunnel Services PIC:n käyttöä, mutta SpiderNet:n J-Series laitteissa näitä ei ole, joten minun tarvitsi määrittää VPLS-protokollaan, ettei se käytä Tunnel Service:ä komennolla *set no-tunnel-services*. Tämän jälkeen tarvitsi luoda tarvittavat Site:t ja määrittää niille *site-identifier* ja siihen kuuluva looginen rajapinta.

Seuraavaksi täytyi konfiguroida BGP-protokolla PE-laitteiden välille käyttämään l2vpn-signalointia:

root@Juniper-R1# edit protocols bgp group VPLS_BGP
[edit protocols bgp group VPLS_BGP]

root@Juniper-R1# set type internal
root@Juniper-R1# set local-address 172.16.1.1
root@Juniper-R1# set family l2vpn signaling
root@Juniper-R1# set neighbor 172.16.1.3

BGP-konfiguraatioissa tuli määrittää ryhmän tyypiksi sisäinen BGP eli iBGP ja määrittää paikallinen osoite, jona käytin Loopback-rajapinnan osoitetta. Lisäksi tarvitsi määrittää, että kyseisen BGP-ryhmän ”perhe” on *l2vpn signaling* eli BGP-ryhmä hoitaa L2VPN: n signalointia, tässä tapauksessa VPLS:n signalointia. Lopuksi määritin naapuriksi Juniper-R3:n Loopback-rajanpinnan IP-osoitteen, johon VPLS_BGP-ryhmä luo BGP-istunnon.

BGP-signaloinnin toiminnan ja liikenteen todentaminen on nähtävissä kappaleessa 9.2.1.

8.4.2 VPLS LDP-signaloinnilla

LDP-signaloidun VPLS konfiguroiminen poikkeaa BGP-signaloidusta reititysinstanssin ja signalointiprotokollan konfiguraatioiden osalta. Rajapintojen konfiguraatiot ovat täsmälleen samat kuin BGP-signaloinnin tapauksessa.

VPLS-instanssin luominen käyttämään LDP-signalointia:

root@Juniper-R1# edit routing-instance Yritys1_VPLS
[edit routing-instance Yritys1_VPLS]
root@Juniper-R1# set instance-type vpls
root@Juniper-R1# set interface ge-1/0/2.101
root@Juniper-R1# set interface ge-1/0/3.101
root@Juniper-R1# edit protocols vpls
[edit routing-instance Yritys1_VPLS protocols vpls]
root@Juniper-R1# set no-tunnel-services
root@Juniper-R1# set vpls-id 10
root@Juniper-R1# set neighbor 172.16.1.3
root@Juniper-R1# set connectivity-type ce

LDP-signaloidun VPLS-instanssin luominen on kahden toimipisteen välille suoraviivaisempi toimenpide kuin BGP-signaloidun. LDP-signaloidussa VPLS-instanssissa määritetään instanssin tyyppi ja siihen kuuluvat rajapinnat kuten BGP-signaloidussa VPLS-instanssissakin, mutta ero tulee VPLS-protokollan määrityksissä, joissa tarvit-

see määritellä ainoastaan VPLS-ID, naapuri PE-laitteen tunniste ja *connectivity-type ce*. VPLS-ID:llä erotellaan eri VPLS-instanssit. Naapuri PE-laitteen tunniste on sen PE-laitteen Loopback-rajapinnan IP-osoite, mihin toinen asiakkaan toimipiste on kytketty. *Connectivity-type ce* määrittää, että VPLS-yhteys pidetään ylhäällä niin kauan kuin VPLS-instanssiin liitetty rajapinta on ylhäällä.

VPLS-instanssin konfiguroimisen lisäksi tarvitsee LDP-protokollaan lisätä Loopback-rajapinta, mikä mahdollistaa signalointitietojen vaihtumisen LDP:tä käyttäen:

root@Juniper-R1# edit protocols ldp
[edit protocols ldp]
root@Juniper-R1# set interface loopback 0.0

LDP-signaloinnin toiminnan ja liikenteen todentaminen on nähtävissä kappaleessa 9.2.2.

8.5 BGP-reitityksen konfigurointi

8.5.1 Operaattori

Operaattorin BGP-reitityksen konfigurointi käsitti kaksi erillistä osaa: eBGP ja iBGP. Operaattorin ja ”Internetin” yhdistäminen tapahtui käyttäen eBGP-yhteyksiä Juniper-R5:n ja CiscoCore-R1:n sekä Juniper-R4:n ja CiscoCore-R3:n välillä. Operaattorin julkisten IP-osoitteiden verkko 130.100.0.0/16 oli tarkoitus mainostaa yhtenä suurena kokonaisuutena Juniper-R4- ja Juniper-R5-laitteilta, joiden reittitauluissa olisi tarkemmat eli pienemmät reittitiedot mm. Yritys1:hen julkiseen verkkoalueeseen.

Operaattorin sisällä käytin reittitietojen jakamiseen iBGP-yhteyksiä, joiden vähentämisen varmistamiseen käytin reittiheijastimina Juniper-R4- ja Juniper-R5-reitittimia. Vaikka näin pienessä verkossa ei reittiheijastimista saada suurempaa hyötyä, oli tärkeää kuitenkin tutkia niiden toiminta sekä konfigurointi.

eBGP-yhteyden muodostaminen CiscoCore-R1:een Juniper-R5:stä

eBGP-yhteyden konfiguroimisessa käytän esimerkkinä Juniper-R5:n ja CiscoCore-R1:n välisen yhteyden luomista Juniper-R5:ssa:

root@Juniper-R5# edit protocols bgp group AS_101
[edit protocols bgp group AS_101]
root@Juniper-R5# set type external
root@Juniper-R5# set local-address 210.10.1.5
root@Juniper-R5# set export advertise_only_aggregate
root@Juniper-R5# set peer-as 101
root@Juniper-R5# set neighbor 210.10.1.6

Ylläolevissa konfiguraatioissa määritettiin käytettävä BGP-ryhmä, jolle määritettiin tyypiksi *external* ja paikalliseksi osoitteeksi ge-1/0/2-rajapinnan IP-osoite. Määritettiin, että mainostusviesteihin käytetään *advertise_only_aggregate*-politiikkaa. Lisäksi määritettiin naapurin AS-numero sekä naapurin IP-osoite, joka on eBGP:n tapauksessa useimmiten linkkivälin IP-osoite. Lisäksi tarvitsi määrittää politiikka, jonka perusteella reitit lisätään BGP-reittipäivityksiin:

root@Juniper-R5# edit policy-options policy-statement advertise_only_aggregate
[edit policy-options policy-statement advertise_only_aggregate]
root@Juniper-R5# edit term 1
[edit policy-options policy-statement advertise_only_aggregate term 1]
root@Juniper-R5# set from protocol aggregate
root@Juniper-R5# set then accept
root@Juniper-R5# up edit term 2
[edit policy-options policy-statement advertise_only_aggregate term 2]
root@Juniper-R5# set from protocol bgp
root@Juniper-R5# set from route-filter 130.100.0.0/16 longer
root@Juniper-R5# set then reject

Ylläolevassa politiikassa määritettiin, että protokollasta *aggregate* tulevat reitit hyväksytään ja protokollasta BGP tulevat reitit joiden verkot ovat 130.100.0.0/16 pienempiä eli omaavat pidemmän verkkomaskin kuin 16. Tämä mahdollisti sen, että sisäisen BGP-ryhmän kautta opitut pienemmät 130.100.0.0-verkot eivät vuoda ”Internetiin” vaan sinne mainostetaan yhtä isoa summaverkkoa. Politiikkaa varten tarvitsi vielä luoda summaverkko routing-options:n alle sekä eBGP-reititystä varten määrittää routing-options-hierarkiatasolle autonomisen alueen tunniste:

root@Juniper-R5# edit routing-options aggregate
[edit routing-options aggregate]
root@Juniper-R5# set route 130.100.0.0/16
root@Juniper-R5# up set autonomous-system 100

Reittiheijastimen konfigurointi Juniper-R5:een

Juniper-R4- ja Juniper-R5-reitittimet toimivat verkossa myös reittiheijastimina iBGP-yhteyksille. Muodostin reitittimistä yhden klusterin, koska käytettäessä Loopback-rajapintojen IP-osoitteita ei ole järkevää muodostaa useita erillisiä klustereita. Reittiheijastimen konfigurointiin tarvitsee vain määrittää iBGP-ryhmälle BGP-tyyppi, mainostuksen rajaava politiikka, cluster-tunniste ja iBGP-naapurit:

root@Juniper-R5# edit protocols bgp group Inter_BGP
[edit protocols bgp group Inter_BGP]
root@Juniper-R5# set type internal
root@Juniper-R5# set cluster 1.2.3.4
root@Juniper-R5# set export external_import
root@Juniper-R5# set neighbor 172.16.1.1
root@Juniper-R5# set neighbor 172.16.1.3
root@Juniper-R5# set neighbor 172.16.1.4

iBGP-reitityksen muodostaminen Juniper-R1:ssä

Sisäisen BGP-reitityksen konfiguroimisessa käytän esimerkkinä Juniper-R1:n konfiguraatioita, koska siellä on myös lisänä asiakkaiden lisääminen BGP-reititykseen:

root@Juniper-R1# edit protocols bgp group Inter_BGP
[edit protocols bgp group Inter_BGP]
root@Juniper-R1# set type internal
root@Juniper-R1# set local-address 172.16.1.1
root@Juniper-R1# set export static_to_bgp
root@Juniper-R1# set export connected_to_bgp
root@Juniper-R1# set neighbor 172.16.1.4
root@Juniper-R1# set neighbor 172.16.1.5

Ensimmäisenä määritettiin BGP-ryhmä Inter_BGP, jolle määritin tyypiksi *internal* ja paikalliseksi osoitteeksi Loopback-rajapinnan osoitteen 172.16.1.1. Lisäksi määritin politiikat, joita käytetään BGP-mainosviestien sisällön rajaamiseen, ja reittiheijastimien IP-osoitteet naapureiksi. Alla on esitetty politiikkojen konfigurointi, missä tuodaan

BGP-reititykseen staattiset reitit ja kytketyistä verkoista 130.100.0.0/16 tai pienemmät verkot:

root@Juniper-R1# edit policy-options policy-statement static_to_bgp
[edit policy-options policy-statement static_to_bgp]
root@Juniper-R1# edit term 1
[edit policy-options policy-statement static_to_bgp term 1]
root@Juniper-R1# set from protocol static
root@Juniper-R1# set then accept

root@Juniper-R1# edit policy-options policy-statement connected_to_bgp
[edit policy-options policy-statement connected_to_bgp]
root@Juniper-R1# edit term 1
[edit policy-options policy-statement connected_to_bgp term 1]
root@Juniper-R1# set from protocol direct
root@Juniper-R1# set from route-filter 130.100.0.0/16 orlonger
root@Juniper-R1# set then accept

Lisäksi tarvitsi määrittää staattinen reitti Yritys1:den julkiseen verkkoon, joka on 130.100.10.0/24:

root@Juniper-R1# edit routing-options static
[edit routing-options static]
root@Juniper-R1# set route 130.100.10.0/24 next-hop 130.100.8.2

8.5.2 “Internet”

”Internetin” konfiguroinnin pyrin pitämään mahdollisimman selkeänä. Kukin Cisco-Core-reititin muodosti oman autonomisen alueen, jonka verkkoja Loopback-rajapinnat simuloivat. BGP-konfiguraatio oli myös yksinkertaisin mahdollinen, koska tarkoituksenani ei ollut tutkia Ciscon menetelmiä BGP-reitityksen toteuttamiseen ainoastaan varmistaa, että ”Internetistä” olisi yhteydellisyys VPLS-asiakkaan verkkoon ja päinvastoin.

Esimerkkinä CiscoCore-R1:den eli AS 101:n konfiguraatiot:

interface Loopback1
ip address 80.0.0.1 255.255.128.0
!
interface Loopback2
ip address 85.0.128.1 255.255.224.0

```
!
interface FastEthernet3/0
 no switchport
 ip address 210.10.1.13 255.255.255.252
!
interface FastEthernet3/3
 description Link to Juniper-R5, port Ge-1/0/2
 no switchport
 ip address 210.10.1.6 255.255.255.252
!
interface GigabitEthernet3/0
 no switchport
 ip address 210.10.1.9 255.255.255.252
!
router bgp 101
 no synchronization
 bgp log-neighbor-changes
 network 80.0.0.0 mask 255.255.128.0
 network 85.0.128.0 mask 255.255.224.0
 neighbor 210.10.1.5 remote-as 100
 neighbor 210.10.1.10 remote-as 106
 neighbor 210.10.1.14 remote-as 102
 no auto-summary
!
```

Ylläolevissa konfiguraatioissa määritin tarvittavien rajapintojen IP-osoitteet sekä BGP-reititysprosessin 101:n, johon liitin Loopback-rajapintojen verkot sekä määritin naapuri-AS:t.

“Internetin” eli CiscoCore-reitittimien kokonaiset konfiguraatiot löytyvät liitteistä 17 - 22.

8.5.3 Yritys1:n konfigurointi

Yritys1:n toimipisteinä toimivat SpiderNet:n WorkGroup:t yksi ja kaksi. WorkGroup1 muodosti yrityksen pääkonttorin, jonka kautta myös muiden toimipisteiden liikenteen reititys ulkoverkkoon tapahtui. Yritys1:n reunareititintä työssä simuloi WG1-SW1, joka on toiminnaltaan L2/L3-kytkin. Määritin kytkimeen tarvittavat VLAN:t sisäverkon IP-osoitteilla sekä kaksi VLAN:ia, jotka muodostivat liityntäverkon Operaattorin PE-laitteen välille (VLAN 1001) ja Yritys1:n julkisen verkon laitteiden reititysrajanpinnan (VLAN 130):

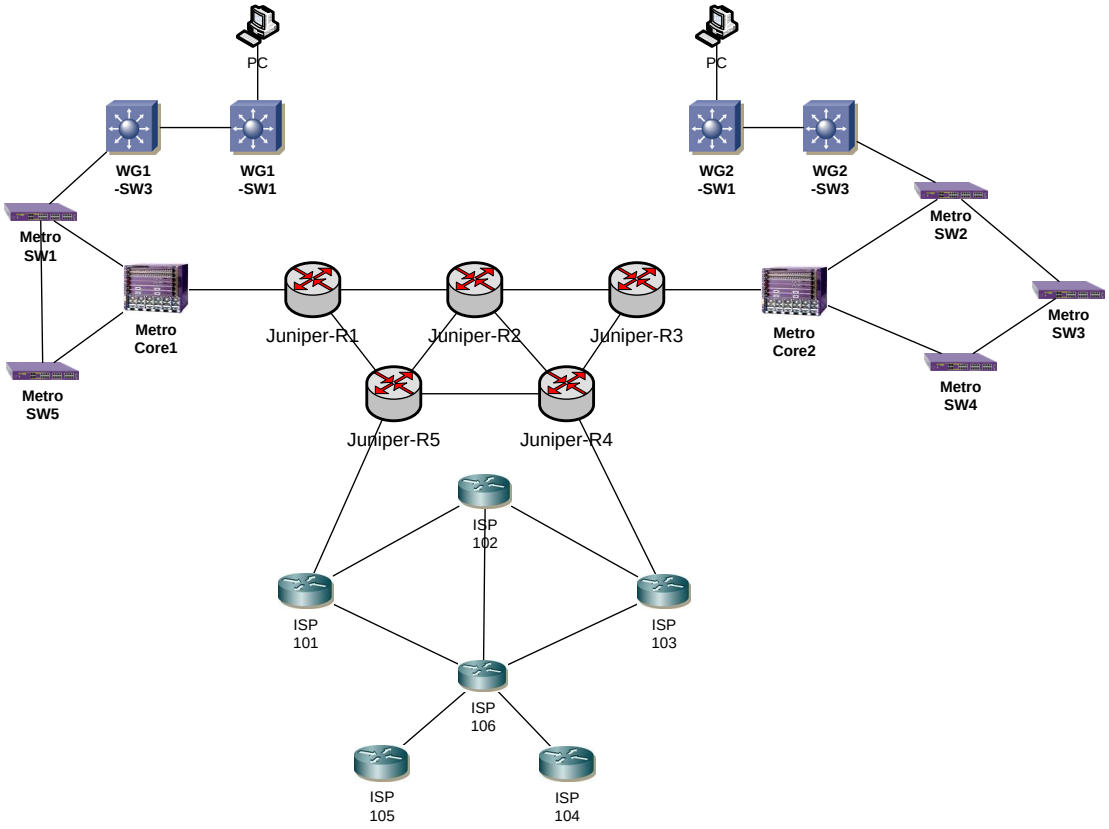
```
vlan 10
 name VLAN10
!
vlan 20
 name VLAN20
!
vlan 130
 name Vlan130
!
vlan 1001
 name Vlan1001
!
interface GigabitEthernet0/3
 description Trunk to WG1-sw3, port 1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/7
 switchport mode access
 switchport access vlan 10
!
interface Vlan10
 description Routing interface for VLAN10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 description Routing interface for VLAN20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan130
 description Public IP routing interface
 ip address 130.100.10.1 255.255.255.0
!
interface Vlan1001
 description Network between Operator
 ip address 130.100.8.2 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 130.100.8.1
```

Yrityksen ”Internetiin” menevä liikenne siis leimataan VLAN-tunnisteella 1001, jonka perusteella Operaattori vie liikenteen reititykseen VPLS-alueen sijasta. Yritys1:n konfiguraatiot ovat nähtävissä liitteissä 23 - 26

9 TYÖN TULOKSET

9.1 Yleistä ja runkoverkonreititys

Työn tuloksena saatiin laboratorioympäristöön nähden erittäin laaja operaattoriverkko, johon sain implementoitua useita verkko-operaattorien käyttämiä tekniikoita ja toimintamalleja Metro Ethernet -alueista, runkoverkon MPLS:ään ja VPLS-L2VPN:ään. Toteutunut verkkotopologia on nähtävissä kuviossa 41, jossa on kuvattuna kaikki työssä käytetyt laitteet ja liitännät.



KUVIO 41. Koko verkon topologia

Runkoverkon IGP-reitityksen ja MPLS:n toiminta on nähtävissä kuvioissa 42 ja 43, jossa on Juniper-R1:n reittitaulu IGP:n, BGP:n ja LDP:n osalta.

```
root@Juniper-R1> show route

inet.0: 28 destinations, 38 routes (28 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/24         *[Direct/0] 1w0d 00:51:45
                     > via ge-1/0/0.0
10.0.0.1/32         *[Local/0] 3w0d 19:59:50
                       Local via ge-1/0/0.0
10.0.1.0/24         *[OSPF/10] 00:14:14, metric 2
                     > to 10.0.0.2 via ge-1/0/0.0
10.0.2.0/24         *[OSPF/10] 00:13:19, metric 3
                       to 10.0.0.2 via ge-1/0/0.0
                     > to 10.0.4.2 via ge-1/0/1.0
10.0.3.0/24         *[OSPF/10] 1d 07:05:59, metric 2
                     > to 10.0.4.2 via ge-1/0/1.0
10.0.4.0/24         *[Direct/0] 3w0d 19:59:47
                     > via ge-1/0/1.0
10.0.4.1/32         *[Local/0] 3w0d 19:59:50
                       Local via ge-1/0/1.0
10.0.5.0/24         *[OSPF/10] 1d 07:05:59, metric 2
                       to 10.0.0.2 via ge-1/0/0.0
                     > to 10.0.4.2 via ge-1/0/1.0
10.0.6.0/24         *[OSPF/10] 1d 20:09:51, metric 2
                     > to 10.0.0.2 via ge-1/0/0.0
12.0.0.0/8          *[BGP/170] 13:26:54, localpref 100, from 172.16.1.4
                       AS path: 103 102 I
                     > to 10.0.4.2 via ge-1/0/1.0, Push 300352
                     [BGP/170] 13:25:55, localpref 100, from 172.16.1.5
                       AS path: 101 102 I
                     > to 10.0.4.2 via ge-1/0/1.0
30.10.0.0/16        *[BGP/170] 13:27:24, localpref 100, from 172.16.1.4
                       AS path: 103 106 105 I
                     > to 10.0.4.2 via ge-1/0/1.0, Push 300352
                     [BGP/170] 13:27:24, localpref 100, from 172.16.1.5
                       AS path: 103 106 105 I
                     > to 10.0.4.2 via ge-1/0/1.0
80.0.0.0/17         *[BGP/170] 13:25:55, MED 0, localpref 100, from 172.16.1.5
                       AS path: 101 I
                     > to 10.0.4.2 via ge-1/0/1.0
                     [BGP/170] 13:25:55, MED 0, localpref 100, from 172.16.1.4
                       AS path: 101 I
                     > to 10.0.4.2 via ge-1/0/1.0, Push 300352
85.0.128.0/19       *[BGP/170] 13:25:55, MED 0, localpref 100, from 172.16.1.5
                       AS path: 101 I
                     > to 10.0.4.2 via ge-1/0/1.0
                     [BGP/170] 13:25:55, MED 0, localpref 100, from 172.16.1.4
                       AS path: 101 I
                     > to 10.0.4.2 via ge-1/0/1.0, Push 300352
100.80.192.0/18     *[BGP/170] 13:26:54, localpref 100, from 172.16.1.4
                       AS path: 103 106 104 I
                     > to 10.0.4.2 via ge-1/0/1.0, Push 300352
                     [BGP/170] 13:26:54, localpref 100, from 172.16.1.5
                       AS path: 103 106 104 I
                     > to 10.0.4.2 via ge-1/0/1.0
130.100.8.0/30      *[Direct/0] 3w0d 19:59:47
                     > via ge-1/0/4.101
130.100.8.1/32      *[Local/0] 3w0d 19:59:50
                       Local via ge-1/0/4.101
130.100.10.0/24     *[Static/5] 1w0d 17:59:53
                     > to 130.100.8.2 via ge-1/0/4.101
150.40.64.0/18      *[BGP/170] 13:27:24, localpref 100, from 172.16.1.4
                       AS path: 103 106 I
                     > to 10.0.4.2 via ge-1/0/1.0, Push 300352
                     [BGP/170] 13:27:24, localpref 100, from 172.16.1.5
                       AS path: 103 106 I
                     > to 10.0.4.2 via ge-1/0/1.0
```

KUVIO 42. Juniper-R1:n reittitaulu osa1 BGP-signaloidun VPLS:n yhteydessä

```
172.16.1.1/32      *[Direct/0] 3w0d 19:59:50
                    > via lo0.0
172.16.1.2/32      *[OSPF/10] 1d 20:09:51, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0
172.16.1.3/32      *[OSPF/10] 00:13:19, metric 2
                    > to 10.0.0.2 via ge-1/0/0.0
172.16.1.4/32      *[OSPF/10] 1d 07:05:59, metric 2
                    > to 10.0.4.2 via ge-1/0/1.0
172.16.1.5/32      *[OSPF/10] 1d 07:05:59, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0
191.145.224.0/19   *[BGP/170] 13:27:24, localpref 100, from 172.16.1.4
                      AS path: 103 106 105 I
                    > to 10.0.4.2 via ge-1/0/1.0, Push 300352
                    [BGP/170] 13:27:24, localpref 100, from 172.16.1.5
                      AS path: 103 106 105 I
                    > to 10.0.4.2 via ge-1/0/1.0
196.197.208.0/20   *[BGP/170] 13:27:24, localpref 100, from 172.16.1.4
                      AS path: 103 106 I
                    > to 10.0.4.2 via ge-1/0/1.0, Push 300352
                    [BGP/170] 13:27:24, localpref 100, from 172.16.1.5
                      AS path: 103 106 I
                    > to 10.0.4.2 via ge-1/0/1.0
200.30.0.0/19      *[BGP/170] 13:27:25, MED 0, localpref 100, from 172.16.1.4
                      AS path: 103 I
                    > to 10.0.4.2 via ge-1/0/1.0, Push 300352
                    [BGP/170] 13:27:25, MED 0, localpref 100, from 172.16.1.5
                      AS path: 103 I
                    > to 10.0.4.2 via ge-1/0/1.0
200.35.0.0/21      *[BGP/170] 13:27:25, MED 0, localpref 100, from 172.16.1.4
                      AS path: 103 I
                    > to 10.0.4.2 via ge-1/0/1.0, Push 300352
                    [BGP/170] 13:27:25, MED 0, localpref 100, from 172.16.1.5
                      AS path: 103 I
                    > to 10.0.4.2 via ge-1/0/1.0
224.0.0.5/32       *[OSPF/10] 3w0d 19:59:50, metric 1
                      MultiRecv

inet.3: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.1.2/32      *[LDP/9] 13:52:32, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0
172.16.1.3/32      *[LDP/9] 00:13:19, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0, Push 300224
172.16.1.4/32      *[LDP/9] 13:52:32, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0, Push 300352
172.16.1.5/32      *[LDP/9] 13:52:32, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0
```

KUVIO 43. Juniper-R1:n reittitaulu osa2 BGP-signaloidun VPLS:n yhteydessä

Kuviot 42 ja 43 varmentavat reitityksen toimivuuden runkoverkossa. Reittitiedot runkoverkon linkkiväleiltä (10.0.x.0/24 verkot) ja Loopback-rajapinnoista (172.16.1.2/32 - 172.16.1.5/32) on välittynyt kaikkialta runkoverkosta Juniper-R1:lle OSPF-reititysprotokollalla. Lisäksi LDP on välittänyt leimatiedot runkoverkon reitittimien Loopback-rajapintoihin.

MPLS:n käyttämät leimat on nähtävissä kuviosta 44, jossa on kuvankaappaus Juniper-R1:n MPLS-reittitaulusta. Koska MPLS-reitittimet oletuksena tekevät Penultimate Hop Popping -toiminnon (PHP), ei MPLS-reittitaulussa näy kuin muutama leimanvaihto eli swap-toiminto ja useita leimanpoisto eli pop-toimintoja. VPLS:ään liittyvän VPLS-leiman 262162 ja Label Switching Instance:n lsi.1071616 käyn tarkemmin läpi 9.2.1-kappaleessa.

```
root@Juniper-R1> show route table mpls.0

mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                  *[MPLS/0] 3w0d 19:56:36, metric 1
                      Receive
1                  *[MPLS/0] 3w0d 19:56:36, metric 1
                      Receive
2                  *[MPLS/0] 3w0d 19:56:36, metric 1
                      Receive
262162             *[VPLS/7] 00:05:54
                    > via lsi.1071616, Pop
302352             *[LDP/9] 13:49:18, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0, Pop
302352(S=0)        *[LDP/9] 13:49:18, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0, Pop
302368             *[LDP/9] 13:49:18, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0, Pop
302368(S=0)        *[LDP/9] 13:49:18, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0, Pop
302384             *[LDP/9] 13:49:18, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0, Swap 300352
302416             *[LDP/9] 00:10:05, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0, Swap 300224
lsi.1071616        *[VPLS/7] 00:05:54, metric2 1
                    > to 10.0.0.2 via ge-1/0/0.0, Push 262153, Push 300224(top)
```

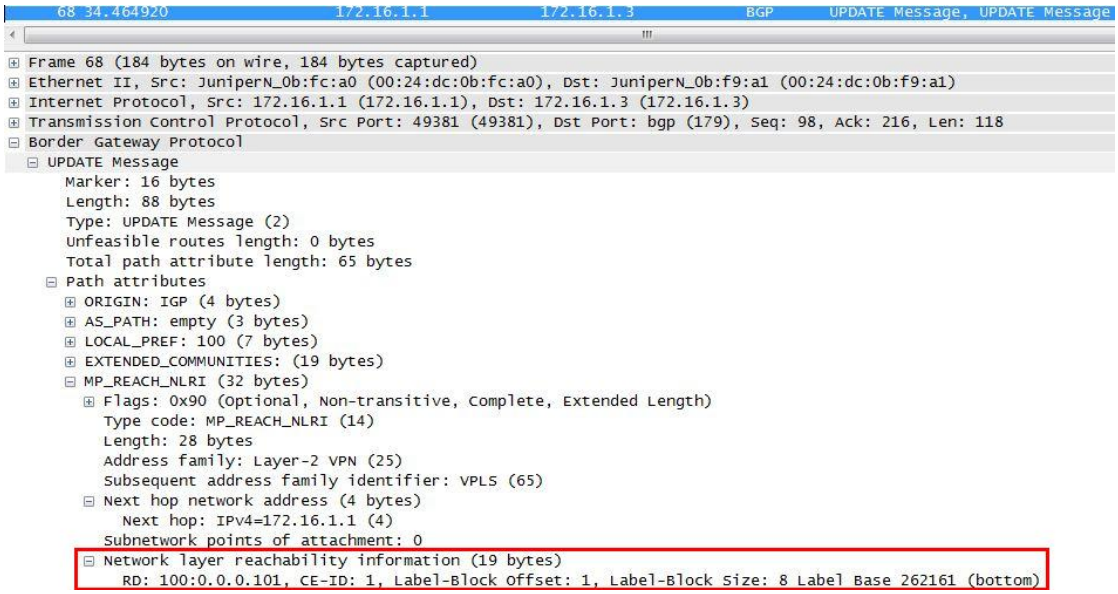
KUVIO 44. Juniper-R1:n MPLS-reittitaulu BGP-signaloidun VPLS:n yhteydessä

9.2 VPLS

9.2.1 BGP-signaloinnin ja asiakasliikenteen todentaminen

VPLS:n BGP-signaloinnin todentamiseen käytin Wireshark-pakettikaappauksia Juniper-R2:n ja Juniper-R3:n väliseltä linkkiväliltä. Pakettikaappauksen otin BGP-naapuruuksien muodostamisen yhteydessä, jolloin myös VPLS-tunnelit signaloidaan PE-laitteiden välille.

Kuviossa 45 on Wireshark-pakettikaappaus Juniper-R1:n BGP-Update-viestistä, jossa Juniper-R1:n lähettää reittipäivityksen omista reiteistään. Update-viestiä edelsi BGP:n naapuruuden muodostukseen käytettävät Open-viestit, joiden esimerkki on BGP:n todentamisosiossa. BGP:n Path attributes -kentässä on pakolliset Well-Known-attribuutit: Origin, AS_Path ja Local_preference. Lisäksi on Multi Protocol -laajennuksen saavutettavuus päivitys eli MP_REACH_NLRI. MP_REACH_NLRI pitää sisällään osoiteperheen tyypin (tässä tapauksessa Layer-2 VPN), tarkempi osoiteperhe tunniste (tässä tapauksessa VPLS), seuraavan hypyn osoite (tässä tapauksessa 172.16.1.1 = Juniper-R1) ja reittitiedot eli NLRI:t.

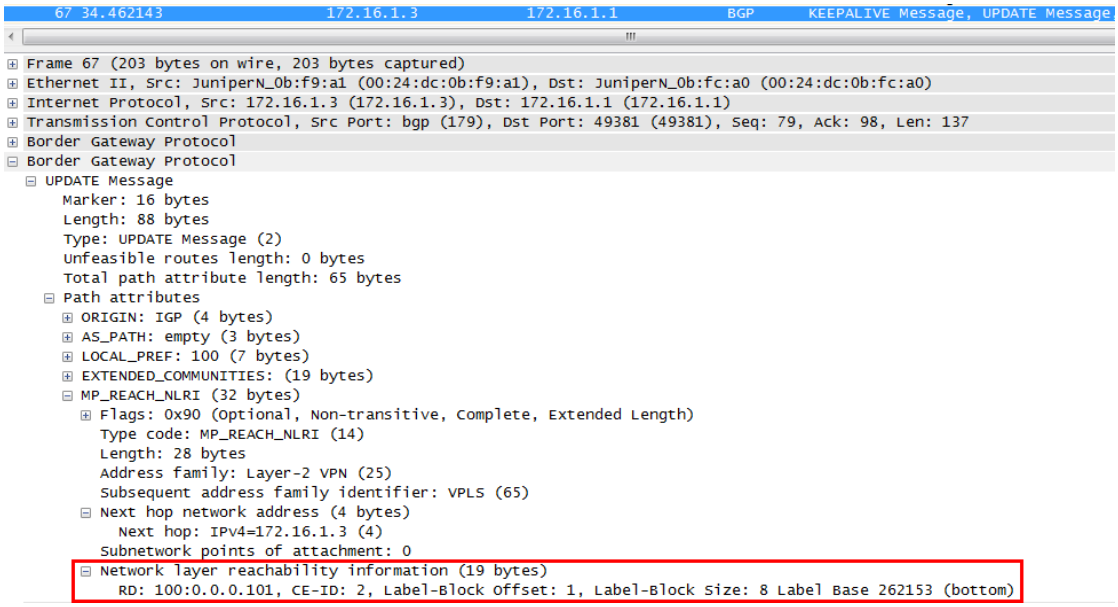


KUVIO 45. BGP-signalointi Juniper-R1:lta Juniper-R3:lle

Kuvion 45 punaisella korostetussa osassa on nähtävissä reittitiedot (NLRI), jotka Juniper-R1 lähettää Juniper-R3:lle. Ensimmäisenä on Route Distinguisher, joksi olin määrittänyt 100:101, mutta se näkyy reittimainostuksessa arvolla 100:0.0.0.101, koska Juniper käyttää RD:n muotona *”AS-numero:IP-osoite”*. Tämän jälkeen on VPLS-konfiguraatio kohdassa määritetty Site-tunniste eli CE-ID arvolla 1, joka vastaa Juniper-R1:n loogista rajapintaa ge-1/0/2.101, jonka siis aikaisemmin määritin kuuluvaksi Yritys1:n VPLS-alueeseen ja Site:ksi 1. Seuraavana on reitittimen luomat Label Block Offset -arvolla 1, Label Block Size -arvolla 8 ja Label Base -leimalla 262161. Kyseiselle reittitiedolle käytettävä leimatieto saadaan laskettua kaavasta: *LB + CE-ID - LBO*, jossa LB on Label Base, CE-ID on vastaanottavan PE-laitteeseen liitetyn toimipisteen Site-ID ja LBO on Label Block Offset. Tässä tapauksessa siis CE-ID:n 1 tavoittamiseksi käytettävä leimatieto on: 262161 + 2 - 1 = 262162, kuten kuviosta 44 on nähtävissä. Tämä vastaa täysin RFC 4761:ssä määriteltyä tapaa luoda leimatieto virtuaalilinkkiä varten. Label Base:n avulla siis määritetään käytettävä leimatunniste erottelemaan eri liikenteet PE-laitteiden välillä. *Asiakasliikenteen kulkeminen runkoverkossa ja VPLS:n toiminta PE-laitteessa* -osiossa käyn tarkemmin läpi, miten kyseistä leimatunnistetta käytetään.

Kuviossa 46 on vastaavasti kuvankaappaus Juniper-R3:n lähettämästä BGP-Update-viestistä, jossa se lähettää siihen kytkettyjen verkkojen reittitiedot. Multi Protocol -

laajennus on täysin samanlainen kuin Juniper-R1:n lähettämässä reittimainostusviestissä poislukien seuraavan hypyn IP-osoite ja reittitiedot.



KUVIO 46. BGP-signalointi Juniper-R3:lta Juniper-R1:lle

Kuvion 46 punaisella korostetussa osassa on nähtävissä Juniper-R3:n mainostama reittitieto, jossa on Route Distuinguisher 100:0.0.0.101, Site-tunnisteella 2, Label Block Offset -arvolla 1, Label Block Size -arvolla 8 ja Label Base -leimalla 262153, joka on myös Juniper-R1:n käyttämä leimatieto CE-ID:lle 2.

Kuviossa 47 on kuvankaappaus Yritys1_VPLS-instanssin reittitaulusta, jossa on reittitiedot: 100:101:1:1/96 ja 100:101:2:1/96. Reittitieto 100:101:1:1/96 vastaa Juniper-R1:een määritettyä paikallista Yritys1:n VPLS-toimipistettä eli Site:ä 1. Reittitieto 100:101:2:1/96 vastaa Juniper-R3:een määritettyä Yritys1:n VPLS-toimipistettä eli Site:ä 2. Kyseinen reittitieto on opittu IP-osoitteesta 172.16.1.3 ja reitti sinne on 10.0.0.2 sekä ge-1/0/0/0.0 kautta leimanarvolla 300224. Leima 300224 on LDP:llä neuvoteltu leima Juniper-R1:n Loopback-rajapinnan ja Juniper-R3:n Loopback-rajapinnan väliseen liikennöintiin eli IP-osoitteiden 172.16.1.1 ja 172.16.1.3 väliseen liikennöintiin (ks. kuvio 44).

```
root@Juniper-R1> show route table Yritys1_VPLS.l2vpn.0

Yritys1_VPLS.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

100:101:1:1/96
                   *[L2VPN/170/-101] 13:36:25, metric2 1
                      Indirect
100:101:2:1/96
                   *[BGP/170] 00:04:36, localpref 100, from 172.16.1.3
                      AS path: I
                    > to 10.0.0.2 via ge-1/0/0.0, Push 300224
```

KUVIO 47. Juniper-R1:stä Yritys1_VPLS:n L2VPN-reittitaulu

Kuviossa 48 on Juniper-R1:lta otettu kuvankaappaus *show vpls connections extensive* -komennosta. Komennolla nähdään kyseisen laitteen VPLS-yhteydet. Kuviosta 48 on nähtävissä seuraavat asiat:

- VPLS-instanssin nimi: *Yritys1_VPLS*
- Paikallinen Site: *Yritys1_WG1*
- Paikallisten rajapintojen määrä: *2*
- Paikalliset rajapinnat: *Ge-1/0/2.101* ja *Ge-1/0/3.101*
- Label Switching Instance eli leimakytkentäinstanssi: *lsi.1071616*
- Käytettävä Label Base: *262161*
- Käytettävä Label Offset: *1*
- Käytettävä Label Range: *8*
- Käytettävä BGP:n Local Preference -arvo: *100* (Oletusarvo)
- Etätoimipisteen eli Remote Site:n arvo: *2*
- Etä-PE-laitteen IP-osoite: *Remote PE: 172.16.1.3*
- Tulevan liikenteen leiman arvo: *Incoming label: 262162*
- Lähtevän liikenteen leiman arvo: *Outgoing label: 262153*
- Paikallisen VPLS-instanssin rajapinta, tilanne ja kapselointitapa: *Local interface: lsi.1071616, Status: Up, Encapsulation: VPLS*
- Yhteyden historiatietoja

```
root@Juniper-R1> show vpls connections extensive
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down    NP -- interface hardware not present
CM -- control-word mismatch      -> -- only outbound connection is up
CN -- circuit not provisioned    <- -- only inbound connection is up
OR -- out of range               Up -- operational
OL -- no outgoing label          Dn -- down
LD -- local site signaled down   CF -- call admission control failure
RD -- remote site signaled down  SC -- local and remote site ID collision
LN -- local site not designated  LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status  IL -- no incoming label
MM -- MTU mismatch               MI -- Mesh-Group ID not availble
BK -- Backup connection          ST -- Standby connection
PF -- Profile parse failure      PB -- Profile busy

Legend for interface status
Up -- operational
Dn -- down

Instance: Yritys1_VPLS
  Local site: Yritys1_WG1 (1)
    Number of local interfaces: 2
    Number of local interfaces up: 2
    IRB interface present: no
    ge-1/0/2.101
    ge-1/0/3.101
    lsi.1071616         2          Intf - vpls Yritys1_VPLS local site 1 remote s
ite 2
    Label-base        Offset     Range      Preference
    262161            1          8          100
    connection-site           Type  St     Time last up          # Up trans
    2                         rmt   Up     Oct 29 13:40:00 2009           1
      Remote PE: 172.16.1.3, Negotiated control-word: No
      Incoming label: 262162, Outgoing label: 262153
      Local interface: lsi.1071616, Status: Up, Encapsulation: VPLS
        Description: Intf - vpls Yritys1_VPLS local site 1 remote site 2
    Connection History:
        Oct 29 13:40:00 2009  status update timer
        Oct 29 13:40:00 2009  loc intf up                  lsi.1071616
        Oct 29 13:40:00 2009  PE route changed
        Oct 29 13:40:00 2009  Out lbl Update                     262153
        Oct 29 13:40:00 2009  In lbl Update                      262162
        Oct 29 13:40:00 2009  loc intf down
```

KUVIO 48. Juniper-R1:n VPLS-yhteydet BGP-signaloidun VPLS:n yhteydessä

VPLS:n tulvitusryhmät ja statistiikka

Kuviossa 49 on Juniper-R1:n VPLS Flood -taulu, josta on nähtävissä VPLS-instanssien eri tulvitusryhmät mitä VPLS:n yhteydessä käytetään. Tulvitusryhmissä määritellään mihin rajapintoihin tuntematon liikenne tulvitetaan VPLS-instanssin sisällä. Tulvitusryhmillä estetään silmukoiden syntyminen VPLS-instanssin sisälle ja näin varmistetaan verkon toimivuus myös kun kohde MAC-osoite ei ole laitteen tiedossa. VPLS:n tapauksessa tulvitusta tehdään ainoastaan seuraavasti:

- Label Switching Instance:stä (LSI) tuleva tuntematon liikenne tulvitetaan kaikille VPLS Edge (VE) -laitteeseen kytkettyihin asiakasliityntöihin (Customer Edge -laitteisiin).

- Asiakasliitynnästä (CE) tuleva tuntematon liikenne tulvitetaan kaikkiin VE-laitteen asiakasliityntöihin paitsi siihen josta kyseinen liikenne on tullut ja Label Switching Instance:een.

```
root@Juniper-R1> show vpls flood extensive
Name: Yritys1_VPLS
CEs: 2
VEs: 1
  Flood route prefix: 0x50/32
  Flood route type: IFF_FLOOD
  Flood route owner: lsi.1071616
  Flood group name: __ves__
  Flood group index: 0
  Nexthop type: comp
  Nexthop index: 577
    Flooding to:
    Name                Type            NhType          Index
    __all_ces__         Group            comp            553
        Composition: split-horizon
        Flooding to:
        Name                Type            NhType          Index
        ge-1/0/3.101        CE               ucst            560
        ge-1/0/2.101        CE               ucst            555

  Flood route prefix: 0x53/32
  Flood route type: IFF_FLOOD
  Flood route owner: ge-1/0/2.101
  Flood group name: __all_ces__
  Flood group index: 1
  Nexthop type: comp
  Nexthop index: 554
    Flooding to:
    Name                Type            NhType          Index
    __all_ces__         Group            comp            553
        Composition: split-horizon
        Flooding to:
        Name                Type            NhType          Index
        ge-1/0/3.101        CE               ucst            560
        ge-1/0/2.101        CE               ucst            555
    Flooding to:
    Name                Type            NhType          Index
    __ves__             Group            comp            575
        Composition: flood-to-all
        Flooding to:
        Name                Type            NhType          Index
        lsi.1071616         VE               indr            262143

  Flood route prefix: 0x52/32
  Flood route type: IFF_FLOOD
  Flood route owner: ge-1/0/3.101
  Flood group name: __all_ces__
  Flood group index: 1
  Nexthop type: comp
  Nexthop index: 554
    Flooding to:
    Name                Type            NhType          Index
    __all_ces__         Group            comp            553
        Composition: split-horizon
        Flooding to:
        Name                Type            NhType          Index
        ge-1/0/3.101        CE               ucst            560
        ge-1/0/2.101        CE               ucst            555
    Flooding to:
    Name                Type            NhType          Index
    __ves__             Group            comp            575
        Composition: flood-to-all
        Flooding to:
        Name                Type            NhType          Index
        lsi.1071616         VE               indr            262143
```

KUVIO 49. Juniper-R1:n VPLS-instanssien tulvitusryhmät

Kuviossa 50 on kuvankaappaus Juniper-R1:n VPLS-statistiikasta, josta nähdään tulvitettujen ja Multicast-liikenteen pakettimäärät sekä MAC-osoitteiden määrät ja rajapinnat, josta ne on opittu.

```
root@Juniper-R1> show vpls statistics
VPLS statistics:

Instance: Yritys1_VPLS
   Local interface: lsi.1071616, Index: 80
   Remote PE: 172.16.1.3
     Current MAC count:                     2
   Local interface: ge-1/0/3.101, Index: 82
     Multicast packets:                   104
     Multicast bytes  :                  6656
     Flooded packets  :                     0
     Flooded bytes    :                     0
     Current MAC count:                     0
   Local interface: ge-1/0/2.101, Index: 83
     Multicast packets:                 24363
     Multicast bytes  :               1755410
     Flooded packets  :                     0
     Flooded bytes    :                     0
     Current MAC count:                     2
```

KUVIO 50. Juniper-R1:n VPLS-statistiikka

Asiakasliikenteen kulkeminen runkoverkossa ja VPLS:n toiminta PE-laitteessa

Asiakkaan toimipisteiden välinen liikenne kuljetetaan runkoverkon läpi käyttäen signaloinnilla muodostettuja tunneleita. Juniper:n käyttämä toteutustapa on käyttää pinottuja MPLS-leimoja. Juniper-reitittimet muodostavat MPLS-leimoja vastaamaan kussakin PE-laitteessa määritettyjä VPLS-toimipisteitä. Reitittimen lähettäessä VPLS-instanssiin kuuluvaa liikennettä runkoverkkoon, se lisää alimmaiseksi leimaksi VPLS-instanssin leiman ja päällimmäiseksi leimaksi leiman, jota käytetään PE-laitteiden väliseen liikennöintiin (usein Loopback-rajapintojen väliseen liikennöintiin).

Kuviossa 51 on kuvankaappaus komennosta *show route forwarding-table family vpls* Juniper-R1:ltä. Komennolla nähdään VPLS-instanssien kytkentätaulut. Kytkentätaulusta on nähtävissä VPLS-instanssin kyseiseen PE-laitteeseen liittyvät rajapinnat ja opitut MAC-osoitteet. MAC-osoitteet ovat VPLS-instanssin ”sisäisiä” MAC-osoitteita eli käytännössä ne ovat asiakas-laitteiden MAC-osoitteita. Esimerkiksi *00:00:e2:9e:3f:9f/48* on reittitieto WG1:een liitettyyn työasemaan. Reittitiedosta nähdään mm., että sen tyyppi on Unicast (ucst) ja rajapinta, jota kautta kyseinen tieto on opittu (ge-1/0/2.101). Reittitieto *00:1e:90:39:7c:e6/48* on Yritys1:n WG2-

toimipisteeseen liitetyn työaseman MAC-osoite. Reittitiedon tyyppi on Indirect (indr) eli se on opittu toiselta PE-laitteelta. Reittitiedon seuraavan hypyn IP-osoite on 10.0.0.2 eli Juniper-R2:n Juniper-R1:een liitetyn rajapinnan IP-osoite. Toimintona kyseiselle reittitiedolle on kaksi Push-toimintoa. Ensimmäisessä Push-toiminnossa lisätään Juniper-R3:n mainostama leima (262153) kyseiselle VPLS-toimipisteelle ja toinen Push-toiminto lisää leiman 300224 päällimmäiseksi leimaksi, joka on LDP:n toimesta muodostettu Juniper-R3:n Loopback-rajapintaa vastaavaksi leimaksi.

```
root@Juniper-R1> show route forwarding-table family vpls
Routing table: Yritys1_VPLS.vpls
VPLS:
Destination        Type RtRef Next hop           Type Index NhRef Netif
default            perm     0                    rjct   569     1
lsi.1071616        user     0                    comp   577     2
ge-1/0/3.101       user     0                    comp   554     3
ge-1/0/2.101       user     0                    comp   554     3
00:00:e2:9e:3f:9f/48
                   dynm     0                    ucst   555     4 ge-1/0/2.101
00:0c:ce:bf:93:03/48
                   dynm     0                    indr 262143     5
                              10.0.0.2          Push 262153, Push 300224(top)
561     2 ge-1/0/0.0
00:0c:ce:bf:99:03/48
                   dynm     0                    ucst   555     4 ge-1/0/2.101
00:1e:90:39:7c:e6/48
                   dynm     0                    indr 262143     5
                              10.0.0.2          Push 262153, Push 300224(top)
561     2 ge-1/0/0.0
```

KUVIO 51. Juniper-R1:n VPLS-kytkentätaulu BGP-signaloidun VPLS:n yhteydessä

Kuviossa 52 on vastaavasti Juniper-R3:n VPLS-kytkentätaulu. Kytkentätaulusta nähdään WG1:ssä olevan työaseman MAC-osoite *00:00:e2:e9:3f:9f* ja sitä vastaava reittitieto *00:00:e2:e9:3f:9f/48*. Juniper-R3:n lähettäessä kehyksen, joka on kohdistettu kyseiseen MAC-osoitteeseen, se lisää alimmaiseksi MPLS-leimaksi Juniper-R1:n VPLS-instanssille käyttämän leiman 262162 ja päällimmäiseksi leimaksi LDP:n muodostaman leiman 300208 (ks. kuvio 53), jota käytetään liikennöintiin Juniper-R1:n Loopback-rajapinnan IP-osoitteeseen 172.16.1.1.

```
root@Juniper-R3> show route forwarding-table family vpls
Routing table: Yritys1_VPLS.vpls
VPLS:
Destination        Type RtRef Next hop           Type Index NhRef Netif
default            perm     0                    rjct   567     1
ge-1/0/2.101       user     0                    comp   573     2
lsi.1074944        user     0                    comp   572     2
00:00:e2:9e:3f:9f/48
                   dynm     0                    indr 262145     7
                              10.0.1.1          Push 262162, Push 300208(top)
542     2 ge-1/0/1.0
00:0c:ce:bf:93:03/48
                   dynm     0                    ucst   544     4 ge-1/0/2.101
00:0c:ce:bf:99:00/48
                   dynm     0                    indr 262145     7
                              10.0.1.1          Push 262162, Push 300208(top)
542     2 ge-1/0/1.0
00:0c:ce:bf:99:03/48
                   dynm     0                    indr 262145     7
                              10.0.1.1          Push 262162, Push 300208(top)
542     2 ge-1/0/1.0
00:1e:90:39:7c:e6/48
                   dynm     0                    ucst   544     4 ge-1/0/2.101
00:24:dc:0b:f9:24/48
                   dynm     0                    indr 262145     7
                              10.0.1.1          Push 262162, Push 300208(top)
542     2 ge-1/0/1.0
```

KUVIO 52. Juniper-R3:n VPLS-kytkentätaulu BGP-signaloidun VPLS:n yhteydessä

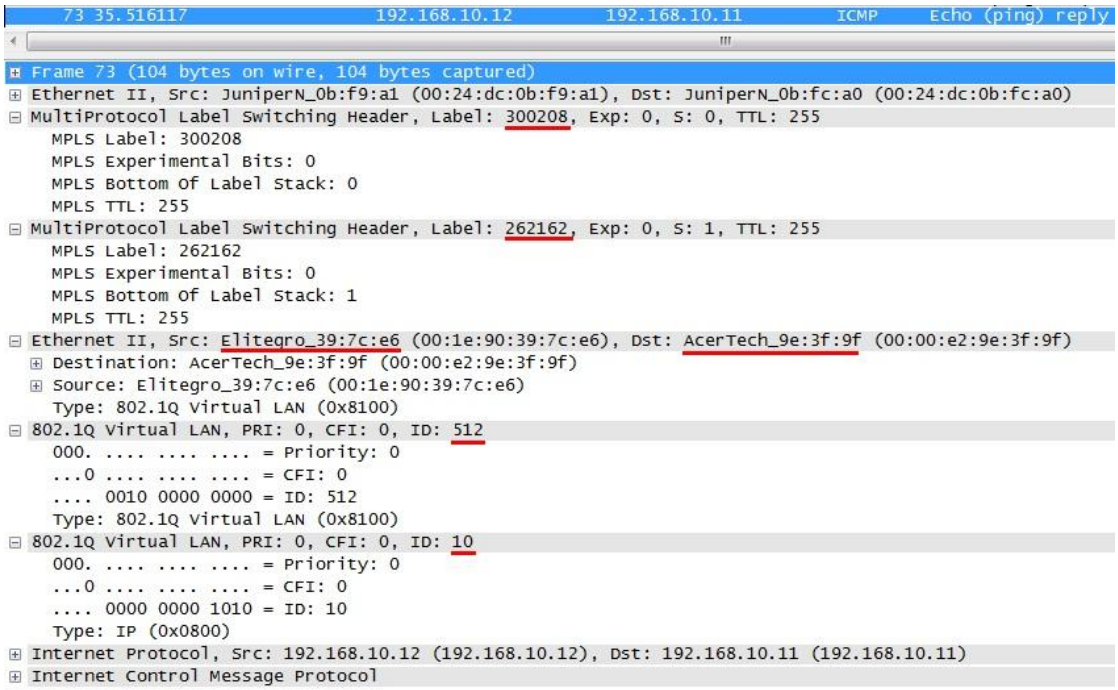
Kuviossa 53 on Juniper-R3:n LDP-leimataulu, josta nähdään runkoverkon reitittimien Loopback-rajapintojen IP-osoitteet ja niitä vastaavat leimatiedot. Juniper-R2:n ja Juniper-R4:n Loopback-rajapintoja ei vastaa mikään leima, koska reitittimet tekevät MPLS:n PHP-toiminnon, jossa ei viimeiselle linkkivälille enää lähetetä MPLS-leimaa.

```
inet.3: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.1.1/32      *[LDP/9] 00:19:01, metric 1
                    > to 10.0.1.1 via ge-1/0/1.0, Push 300208
172.16.1.2/32      *[LDP/9] 00:19:01, metric 1
                    > to 10.0.1.1 via ge-1/0/1.0
172.16.1.4/32      *[LDP/9] 00:19:52, metric 1
                    > to 10.0.2.2 via ge-1/0/0.0
172.16.1.5/32      *[LDP/9] 00:19:01, metric 1
                    > to 10.0.2.2 via ge-1/0/0.0, Push 302576
                      to 10.0.1.1 via ge-1/0/1.0, Push 299776
```

KUVIO 53. Juniper-R3:n LDP-leimataulu BGP-signaloidun VPLS:n yhteydessä

Kuviossa 54 on Wireshark-pakettikaappaus Juniper-R3:n ja Juniper-R2:n väliseltä linkiltä. Pakettikaappauksessa on Ping Reply -viesti työasemalta, joka on liitetty Yritys1:n toimipisteeseen WG2:ssa, työasemalle, joka on liitetty Yritys1:n toimipisteeseen WG1:ssä.



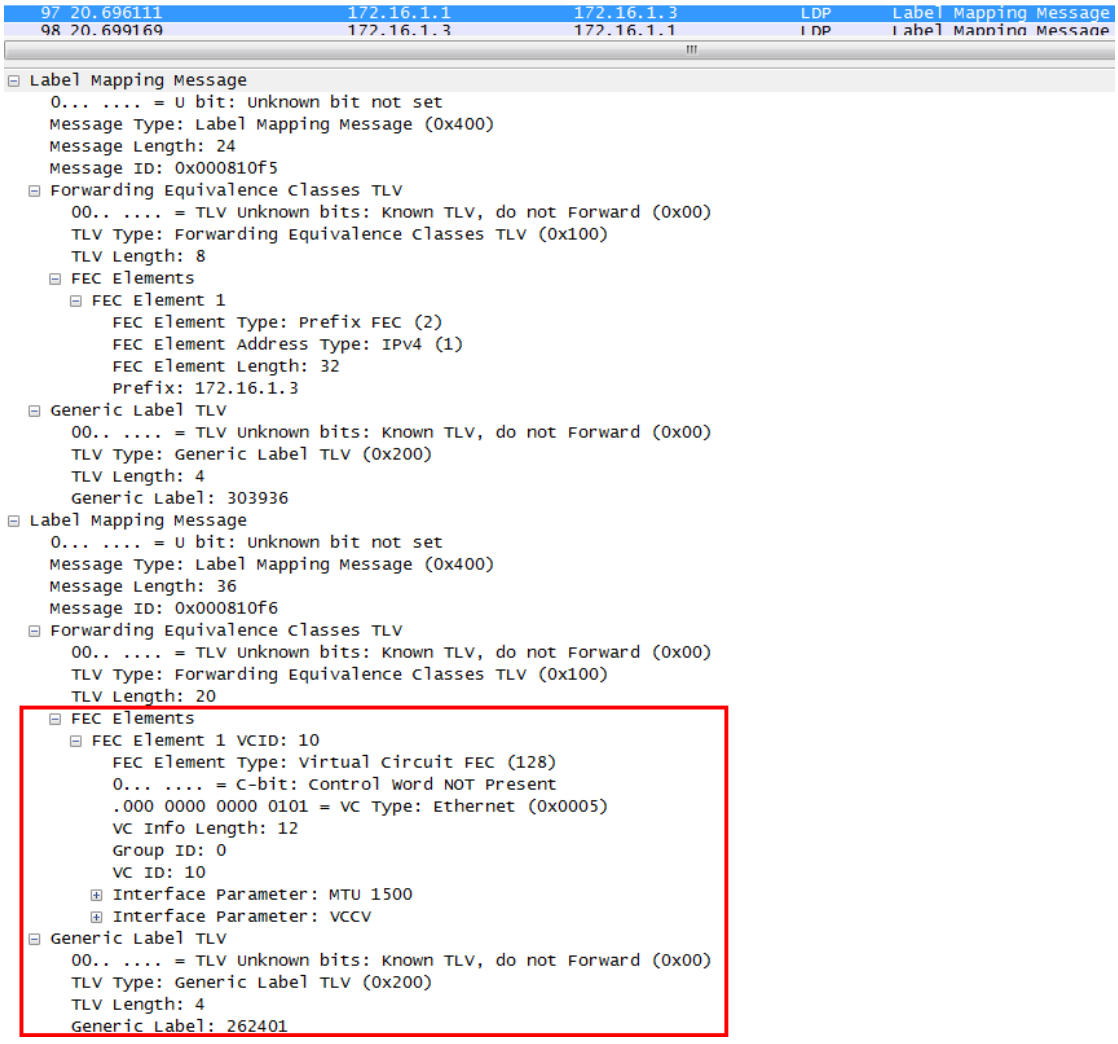
KUVIO 54. Ping WG2:een liitetyltä työasemalta WG1:een liitettyyn työasemaan BGP-signaloidun VPLS:n yhteydessä

Kuviossa 54 on punaisella alleviivattu merkittävimmät osat paketin sisällöstä. Ensimmäisenä on MPLS-leima 300208, joka on Juniper-R1:n Loopback-rajapinnan 172.16.1.1 leimatieto (ks. kuvio 53). Seuraavana on MPLS-leima 262162, joka on muodostettu vastaamaan Juniper-R1:n Yritys1_VPLS-instanssia. Seuraavina on asiakaslaitteiden MAC-osoitteet sekä kaksi VLAN-leimaa, joista ensimmäinen on Metro Ethernet -alueeseen määritetty VMAN-leima 512, jota käytetään erottelemaan Yritys1:n liikenne muusta liikenteestä Metro Ethernet -alueissa. Jälkimmäinen VLAN-leima 10 on asiakkaan sisäverkon leimatieto, jota käytetään asiakkaan verkossa liikenteen erotteluun.

9.2.2 LDP-signaloinnin ja asiakasliikenteen todentaminen

VPLS:n LDP-signaloinnin todentamiseen käytin Wireshark-pakettikaappauksia Juniper-R2:n ja Juniper-R3:n väliseltä linkkiväliltä. Pakettikaappauksen otin naapuruuksien muodostamisen yhteydessä, jolloin myös VPLS-tunnelit signaloidaan PE-laitteiden välille.

Kuviossa 55 on kuvankaappaus Wireshark-pakettikaappauksesta, josta on nähtävissä LDP-viesti. LDP-viestissä on Label Mapping Message (LMM)-viesti, jossa välitetään VPLS:n tietoja. Ensimmäisessä auki olevassa LMM-viestissä Juniper-R1 lähettää Juniper-R3:n Loopback-rajapinnan IP-osoitetta vastaavan leimatiedon (Generic Label 303936), joka on siis Juniper-R1:n käyttämä leima MPLS-polulle, mutta kuten kuviosta 54 on nähtävissä, kyseiselle leimalle on swap-toiminto MPLS-leimataulussa. Swap-toiminto vaihtaa leiman arvon reittitaulussa näkyvään 300336 leimaan, joka vastaa Juniper-R3:n Loopback-rajapinnan IP-osoitetta 172.16.1.3 (ks. kuvio 57). Seuraavassa auki olevassa LMM-viestissä on virtuaalilinkin muodostaminen Juniper-R1:n ja Juniper-R3:n välille. Juniper-R1:n lähettää LMM:n, jossa on FEC TLV, jonka sisällä kuljetetaan FEC Elements -viesti, ja Generic Label TLV -viesti.



KUVIO 55. LDP-signalointi Juniper-R1:lta Juniper-R3:lle

Kuvion 55 punaisella rajatussa alueessa on virtuaalilinkin muodostaminen Juniper-R1:n ja Juniper-R3:n välille. FEC Element -viestissä on FEC Element:n tyyppi, joka on Juniperin käyttämä 128. Seuraavassa määritetään virtuaalilinkin (Virtual Circuit) tyyppi, joka on tässä tapauksessa Ethernet. Lisäksi kuljetetaan VPLS-tunniste (VC-ID), joksi olin määrittänyt LDP-signaloidun VPLS:n yhteydessä arvon 10. VC-ID on käytännössä yhtä kuin VPLS-tunniste, koska jokaista VPLS:ää varten tarvitsee luoda oma virtuaalilinkki PE-laitteiden välille. FEC TLV:n jälkeen on Generic Label TLV, jossa määritetään käytettävä leima kyseiselle virtuaalilinkille. Tässä tapauksessa leiman arvo on 262401.

```
root@Juniper-R1> show route table mpls.0

mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                  *[MPLS/0] 3w4d 19:37:10, metric 1
                      Receive
1                  *[MPLS/0] 3w4d 19:37:10, metric 1
                      Receive
2                  *[MPLS/0] 3w4d 19:37:10, metric 1
                      Receive
262401             *[VPLS/7] 00:03:29
                    > via lsi.1097216, Pop
303888             *[LDP/9] 00:03:44, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0, Pop
303888(S=0)        *[LDP/9] 00:03:44, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0, Pop
303904             *[LDP/9] 00:03:44, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0, Pop
303904(S=0)        *[LDP/9] 00:03:44, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0, Pop
303920             *[LDP/9] 00:03:44, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0, Swap 300352
303936             *[LDP/9] 00:03:44, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0, Swap 300336
lsi.1097216        *[VPLS/7] 00:03:29, metric2 1
                    > to 10.0.0.2 via ge-1/0/0.0, Push 262145, Push 300336(top)
```

KUVIO 56. Juniper-R1:n MPLS-reittitaulu LDP-signaloidun VPLS:n yhteydessä

```
inet.3: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.1.2/32      *[LDP/9] 00:04:58, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0
172.16.1.3/32      *[LDP/9] 00:04:58, metric 1
                    > to 10.0.0.2 via ge-1/0/0.0, Push 300336
172.16.1.4/32      *[LDP/9] 00:04:58, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0, Push 300352
172.16.1.5/32      *[LDP/9] 00:04:58, metric 1
                    > to 10.0.4.2 via ge-1/0/1.0
```

KUVIO 57. Juniper-R1:n LDP-leimataulu LDP-signaloidun VPLS:n yhteydessä

Kuviossa 58 on Juniper-R1:n L2Circuit-reittitaulu, josta on nähtävissä VPLS:n käyttämät VPLS-reittitiedot. Ensimmäisenä on *172.16.1.3:NoCtrlWord:5:10:Local/96*,

joka tarkoittaa Juniper-R3:n Loopback-rajapintaan muodostettua tunnelia, jonka ulommaisena LDP-leimana käytetään leimaa 300336. Toinen reittitieto on edellisen reittitiedon Remote-versio, joka hylätään.

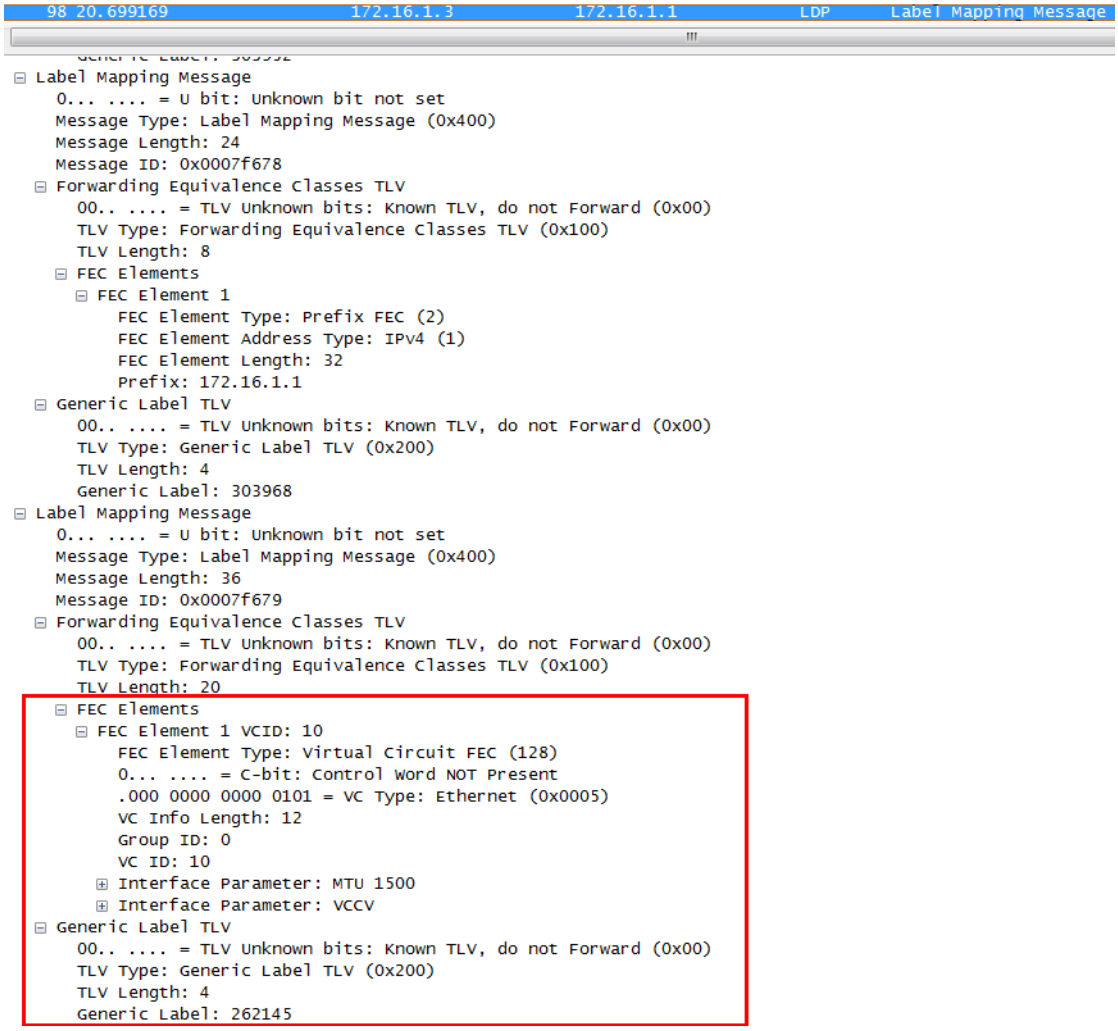
```
root@Juniper-R1> show route table l2circuit.0

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.1.3:NoCtrlWord:5:10:Local/96
                   *[VPLS/7] 20:06:47, metric2 1
                    > to 10.0.0.2 via ge-1/0/0.0, Push 300336
172.16.1.3:NoCtrlWord:5:10:Remote/96
                   *[LDP/9] 00:03:51
                      Discard
```

KUVIO 58. Juniper-R1:n L2Circuit-reittitaulu

Kuviossa 59 on kuvankaappaus Wireshark-pakettikaappauksesta, josta on nähtävissä LDP-viesti. LDP-viestissä on Label Mapping Message (LMM)-viesti, jossa välitetään VPLS:n tietoja. Ensimmäisessä auki olevassa LMM-viestissä Juniper-R3 lähettää Juniper-R1:n Loopback-rajapinnan IP-osoitetta vastaavan leimatiedon (Generic Label 303968), joka on siis Juniper-R3:n käyttämä leima MPLS-polulle, mutta kuten kuviosta 60 on nähtävissä, kyseiselle leimalle on swap-toiminto MPLS-leimataulussa. Swap-toiminto vaihtaa leiman arvon reittitaulussa näkyvään 300240 leimaan, joka vastaa Juniper-R1:n Loopback-rajapinnan IP-osoitetta 172.16.1.1 (ks. kuvio 61). Seuraavassa auki olevassa LMM-viestissä on virtuaalilinkin muodostaminen Juniper-R3:n ja Juniper-R1:n välille. Juniper-R3:n lähettää LMM:n, jossa on FEC TLV, jonka sisällä kuljetetaan FEC Elements -viesti, ja Generic Label TLV -viesti.



KUVIO 59. LDP-signalointi Juniper-R3:lta Juniper-R1:lle

Kuvion 59 punaisella rajatussa osassa on FEC Elements- ja Generic Label TLV -viestit.FEC Elements -viestissä on määritetty FEC Element:n tyypiksi 128 ja VC-ID:ksi 10, joka on siis VPLS-tunniste Yritys1:n VPLS:lle. Generic Label TLV -viestissä on kyseisen VPLS:instanssin LDP-leiman arvo 262145.

```
root@Juniper-R3> show route table mpls.0

mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                  *[MPLS/0] 3w4d 15:45:39, metric 1
                      Receive
1                  *[MPLS/0] 3w4d 15:45:39, metric 1
                      Receive
2                  *[MPLS/0] 3w4d 15:45:39, metric 1
                      Receive
262145             *[VPLS/7] 00:07:13
                    > via lsi.1103616, Pop
303920             *[LDP/9] 00:07:28, metric 1
                    > to 10.0.2.2 via ge-1/0/0.0, Pop
303920(S=0)        *[LDP/9] 00:07:28, metric 1
                    > to 10.0.2.2 via ge-1/0/0.0, Pop
303936             *[LDP/9] 00:07:28, metric 1
                      to 10.0.2.2 via ge-1/0/0.0, Swap 302576
                    > to 10.0.1.1 via ge-1/0/1.0, Swap 299776
303952             *[LDP/9] 00:07:28, metric 1
                    > to 10.0.1.1 via ge-1/0/1.0, Pop
303952(S=0)        *[LDP/9] 00:07:28, metric 1
                    > to 10.0.1.1 via ge-1/0/1.0, Pop
303968             *[LDP/9] 00:07:28, metric 1
                    > to 10.0.1.1 via ge-1/0/1.0, Swap 300240
lsi.1103616        *[VPLS/7] 00:07:13, metric2 1
                    > to 10.0.1.1 via ge-1/0/1.0, Push 262401, Push 300240(top)
```

KUVIO 60. Juniper-R3:n MPLS-reittitaulu LDP-signaloidun VPLS:n yhteydessä

```
inet.3: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.1.1/32      *[LDP/9] 00:08:47, metric 1
                    > to 10.0.1.1 via ge-1/0/1.0, Push 300240
172.16.1.2/32      *[LDP/9] 00:08:47, metric 1
                    > to 10.0.1.1 via ge-1/0/1.0
172.16.1.4/32      *[LDP/9] 00:08:47, metric 1
                    > to 10.0.2.2 via ge-1/0/0.0
172.16.1.5/32      *[LDP/9] 00:08:47, metric 1
                      to 10.0.2.2 via ge-1/0/0.0, Push 302576
                    > to 10.0.1.1 via ge-1/0/1.0, Push 299776
```

KUVIO 61. Juniper-R3:n LDP-leimataulu LDP-signaloidun VPLS:n yhteydessä

Kuviossa 62 on Juniper-R1:lta otettu kuvankaappaus show vpls connections extensive -komennosta. Komennolla nähdään kyseisen laitteen VPLS-yhteydet. Kuviosta 62 on nähtävissä seuraavat asiat:

- VPLS-instanssin nimi: *Yritys1_VPLS*
- VPLS-ID: *10*
- Paikallisten rajapintojen määrä: *2*
- Paikalliset rajapinnat: *Ge-1/0/2.101 ja Ge-1/0/3.101*
- Label Switching Instance eli leimakytkentäinstanssi: *lsi.1097216*
- Naapuri-PE-laitteen IP-osoite ja VPLS-ID: *172.16.1.3 (vpsl-id 10)*

- Kyseiseen naapuruuteen liittyvät leimat sekä sisääntulevalle että lähtevälle liikenteelle: *Incoming label: 262401, Outgoing label: 262145*
- Paikallisen VPLS-instanssin rajapinta, tilanne ja kapselointitapa: *Local interface: lsi.1097216, Status: Up, Encapsulation: ETHERNET*
- Yhteyden historiatietoja

```
root@Juniper-R1> show vpls connections extensive
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down    NP -- interface hardware not present
CM -- control-word mismatch      -> -- only outbound connection is up
CN -- circuit not provisioned    <- -- only inbound connection is up
OR -- out of range               Up -- operational
OL -- no outgoing label          Dn -- down
LD -- local site signaled down   CF -- call admission control failure
RD -- remote site signaled down  SC -- local and remote site ID collision
LN -- local site not designated  LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status  IL -- no incoming label
MM -- MTU mismatch               MI -- Mesh-Group ID not availble
BK -- Backup connection          ST -- Standby connection
PF -- Profile parse failure      PB -- Profile busy

Legend for interface status
Up -- operational
Dn -- down

Instance: Yritys1_VPLS
  VPLS-id: 10
    Number of local interfaces: 2
    Number of local interfaces up: 2
    ge-1/0/2.101
    ge-1/0/3.101
    lsi.1097216                  Intf - vpls Yritys1_VPLS neighbor 172.16.1.3 v
pls-id 10
    Neighbor                Type  St     Time last up          # Up trans
    172.16.1.3(vpls-id 10)  rmt   Up     Nov  2 13:22:59 2009           1
      Remote PE: 172.16.1.3, Negotiated control-word: No
      Incoming label: 262401, Outgoing label: 262145
      Local interface: lsi.1097216, Status: Up, Encapsulation: ETHERNET
        Description: Intf - vpls Yritys1_VPLS neighbor 172.16.1.3 vpls-id 10
    Connection History:
        Nov  2 13:22:59 2009  status update timer
        Nov  2 13:22:59 2009  PE route changed
        Nov  2 13:22:59 2009  In lbl Update                    262401
        Nov  2 13:22:59 2009  Out lbl Update                   262145
        Nov  2 13:22:59 2009  In lbl Update                    262401
        Nov  2 13:22:59 2009  loc intf up                  lsi.1097216
```

KUVIO 62. Juniper-R1:n VPLS-yhteydet

Asiakasliikenteen kulkeminen runkoverkossa ja VPLS:n toiminta PE-laitteessa

Asiakasliikenteen kulkeminen runkoverkossa on täsmälleen vastaavaa LDP-signaloidun VPLS:n tapauksessa kuin on BGP-signaloidun VPLS:n tapauksessa. Juniper-reitittimet käyttävät pinottuja MPLS-leimoja tunneloimaan VPLS-liikenne läpi MPLS-verkon.

Kuviossa 63 on kuvankaappaus komennosta *show route forwarding-table family vpls* Juniper-R1:ltä. Komennolla nähdään VPLS-instanssien kytkentätaulut. Kytkentätaulusta on nähtävissä VPLS-instanssin kyseiseen PE-laitteeseen liittyvät rajapinnat ja opitut MAC-osoitteet. MAC-osoitteet ovat VPLS-instanssin ”sisäisiä” MAC-osoitteita eli käytännössä ne ovat asiakkaan laitteiden MAC-osoitteita. Esimerkiksi *00:00:e2:9e:3f:9f/48* on reittitieto WG1:een liitettyyn työasemaan. Reittitiedosta nähdään mm., että sen tyyppi on Unicast (ucst) ja rajapinta, jota kautta kyseinen tieto on opittu (ge-1/0/2.101). Reittitieto *00:1e:90:39:7c:e6/48* on Yritys1:n WG2-toimipisteeseen liitetyn työaseman MAC-osoite. Reittitiedon tyyppi on Indirect (indr) eli se on opittu toiselta PE-laitteelta. Reittitiedon seuraavan hypyn IP-osoite on 10.0.0.2 eli Juniper-R2:n Juniper-R1:een liitetyn rajapinnan IP-osoite. Toimintona kyseiselle reittitiedolle on kaksi Push-toimintoa. Ensimmäisessä Push-toiminnossa lisätään Juniper-R3:n mainostama leima (262145) kyseiselle VPLS-toimipisteelle ja toinen Push-toiminto lisää leiman 300336 päällimmäiseksi leimaksi, joka on LDP:n toimesta muodostettu Juniper-R3:n Loopback-rajapintaa vastaavaksi leimaksi. Muut reittitiedot ovat Yritys1:n toimipisteiden Cisco-laitteiden MAC-osoitteita.

```
root@Juniper-R1> show route forwarding-table family vpls
Routing table: Yritys1_VPLS.vpls
VPLS:
Destination        Type RtRef Next hop           Type Index NhRef Netif
default            perm     0                    rjct   555     1
ge-1/0/3.101       user     0                    comp   577     3
ge-1/0/2.101       user     0                    comp   577     3
lsi.1097216        user     0                    comp   583     2
00:00:e2:9e:3f:9f/48
                   dynm     0                    ucst   568     5 ge-1/0/2.101
00:0c:ce:bf:93:03/48
                   dynm     0                    indr 262142     5
                              10.0.0.2          Push 262145, Push 300336(top)
580     2 ge-1/0/0.0
00:0c:ce:bf:99:00/48
                   dynm     0                    ucst   568     5 ge-1/0/2.101
00:0c:ce:bf:99:03/48
                   dynm     0                    ucst   568     5 ge-1/0/2.101
00:1e:90:39:7c:e6/48
                   dynm     0                    indr 262142     5
                              10.0.0.2          Push 262145, Push 300336(top)
580     2 ge-1/0/0.0
```

KUVIO 63. Juniper-R1:n VPLS-kytkentätaulu LDP-signaloidun VPLS:n yhteydessä

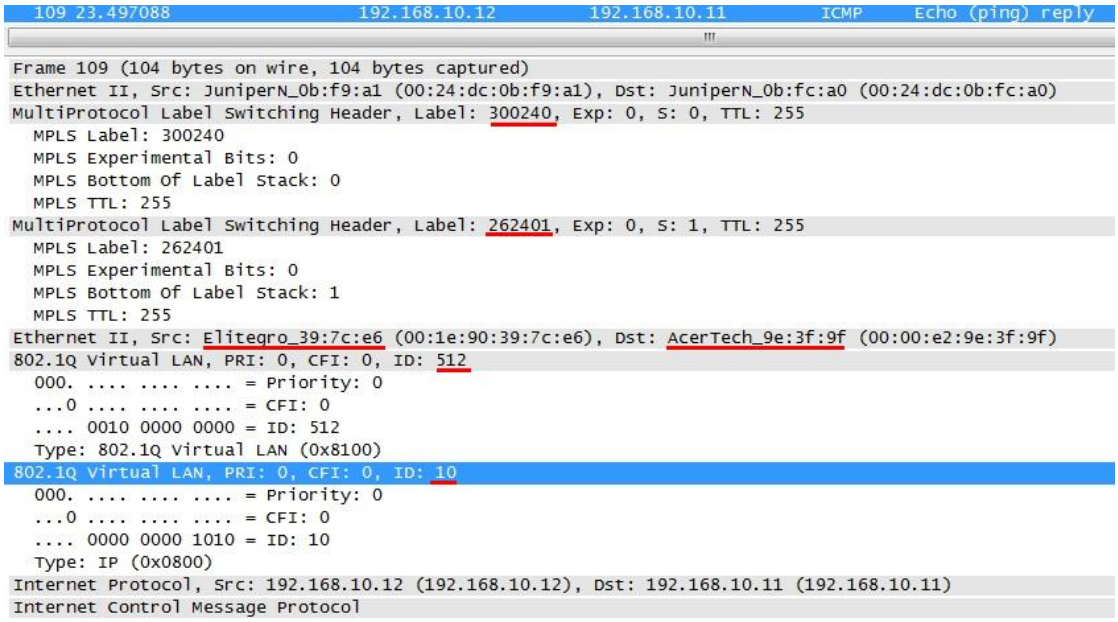
Kuviossa 64 on vastaavasti Juniper-R3:n VPLS-kytkentätaulu. Kytkentätaulusta nähdään WG1:ssä olevan työaseman MAC-osoite *00:00:e2:e9:3f:9f* ja sitä vastaava reittitieto *00:00:e2:e9:3f:9f/48*. Juniper-R3:n lähettäessä kehyksen, joka on kohdistettu kyseiseen MAC-osoitteeseen, se lisää alimmaiseksi MPLS-leimaksi Juniper-R1:n VPLS-instanssille käyttämän leiman 262401 ja päällimmäiseksi leimaksi LDP:n muo-

dostaman leiman 300240 (ks. kuvio 61), jota käytetään liikennöintiin Juniper-R1:n Loopback-rajapinnan IP-osoitteeseen 172.16.1.1.

```
root@Juniper-R3> show route forwarding-table family vpls
Routing table: Yritys1_VPLS.vpls
VPLS:
Destination        Type RtRef Next hop           Type Index NhRef Netif
default            perm     0                    rjct   562     1
ge-1/0/2.101       user     0                    comp   572     2
lsi.1103616        user     0                    comp   573     2
00:00:e2:9e:3f:9f/48
                   dynm     0                    indr 262145     7
                              10.0.1.1          Push 262401, Push 300240(top)
567     2 ge-1/0/1.0
00:0c:ce:bf:93:00/48
                   dynm     0                    ucst   565     5 ge-1/0/2.101
00:0c:ce:bf:93:03/48
                   dynm     0                    ucst   565     5 ge-1/0/2.101
00:0c:ce:bf:99:00/48
                   dynm     0                    indr 262145     7
                              10.0.1.1          Push 262401, Push 300240(top)
567     2 ge-1/0/1.0
00:0c:ce:bf:99:03/48
                   dynm     0                    indr 262145     7
                              10.0.1.1          Push 262401, Push 300240(top)
567     2 ge-1/0/1.0
00:1e:90:39:7c:e6/48
                   dynm     0                    ucst   565     5 ge-1/0/2.101
00:24:dc:0b:f9:24/48
                   dynm     0                    indr 262145     7
                              10.0.1.1          Push 262401, Push 300240(top)
567     2 ge-1/0/1.0
```

KUVIO 64. Juniper-R3:n VPLS-kytkentätaulu LDP-signaloidun VPLS:n yhteydessä

Kuviossa 65 on Wireshark-pakettikaappaus Juniper-R3:n ja Juniper-R2:n väliseltä linkiltä. Pakettikaappauksessa on Ping Reply -viesti työasemalta, joka on liitetty Yritys1:n toimipisteeseen WG2:ssa, työasemalle, joka on liitetty Yritys1:n toimipisteeseen WG1:ssä.



KUVIO 65. Ping WG2:een liitetyltä työasemalta WG1:een liitettyyn työasemaan LDP-signaloidun VPLS:n yhteydessä

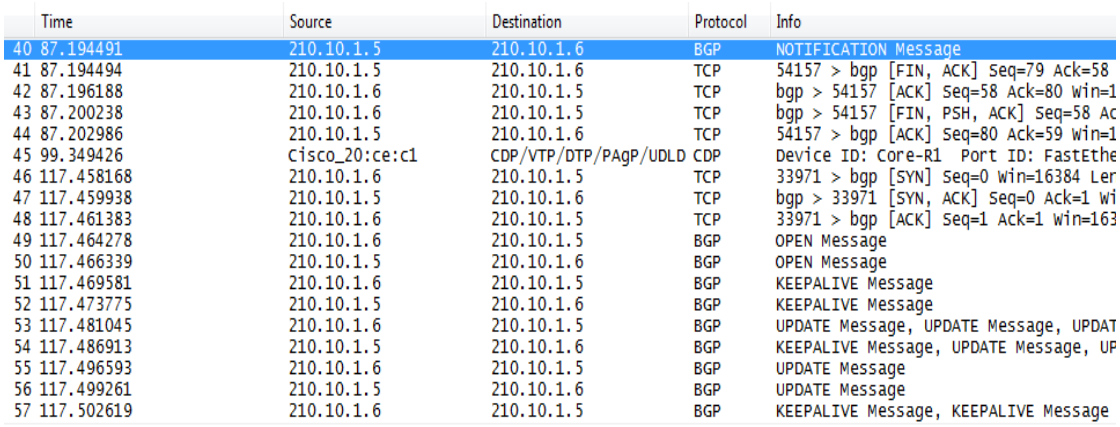
Kuviossa 65 on punaisella alleviivattu merkittävimmät osat paketin sisällöstä. Ensimmäisenä on MPLS-leima 300240, joka on Juniper-R1:n Loopback-rajapinnan 172.16.1.1 leimatieto (ks. kuvio 61). Seuraavana on MPLS-leima 262401, joka on muodostettu vastaamaan Juniper-R1:n Yritys1_VPLS-instanssia. Seuraavina on asiakaslaitteiden MAC-osoitteet sekä kaksi VLAN-leimaa, joista ensimmäinen on Metro Ethernet -alueeseen määritetty VMAN- eli QinQ-leima 512, jota käytetään erottelemaan Yritys1:n liikenne muusta liikenteestä Metro Ethernet -alueissa. Jälkimmäinen VLAN-leima 10 on asiakkaan sisäverkon leimatieto, jota käytetään asiakkaan verkossa liikenteen erotteluun.

9.3 BGP-reitityksen todentaminen

BGP-reitityksen todentamisessa käytin Wireshark-pakettikaappauksia Juniper-R5:n ja CiscoCore-R1:n väliseltä linkkiväliltä. Wireshark-kaappauksien tarkoituksena on havainnollistaa, miten BGP-yhteyden luominen tapahtuu ja mitä eri attribuutteja sekä reittitietoja laitteiden välillä välittyy.

Kuviossa 66 on pakettikaappaus BGP-yhteyden purkamisesta ja uudelleen muodostamisesta Juniper-R5:n ja CiscoCore-R1:n välille. Ensimmäisenä suljettiin yhteys Juni-

per-R5:n toimesta (lähde-IP-osoite=210.10.1.5) Notification-viestillä. Tämän jälkeen reitittimet purkavat TCP-yhteyden ja luovat noin 30s kuluttua uuden TCP-yhteyden. Seuraavana CiscoCore-R1 ja Juniper-R5 lähettävät Open-viestit, joiden jälkeen BGP-yhteys on muodostunut. BGP-yhteyden purkamisen ja uudelleen muodostamisen kesto on noin 30s. Tämän jälkeen BGP-osapuolet lähettävät Keepalive-viestejä, joilla ne varmistavat yhteyden olemassaolon. Yhteyden muodostamisen jälkeen BGP-osapuolet lähettävät Update-viestejä, jotka sisältävät reitittimen BGP-reittitaulussa olevat reitti-tiedot.

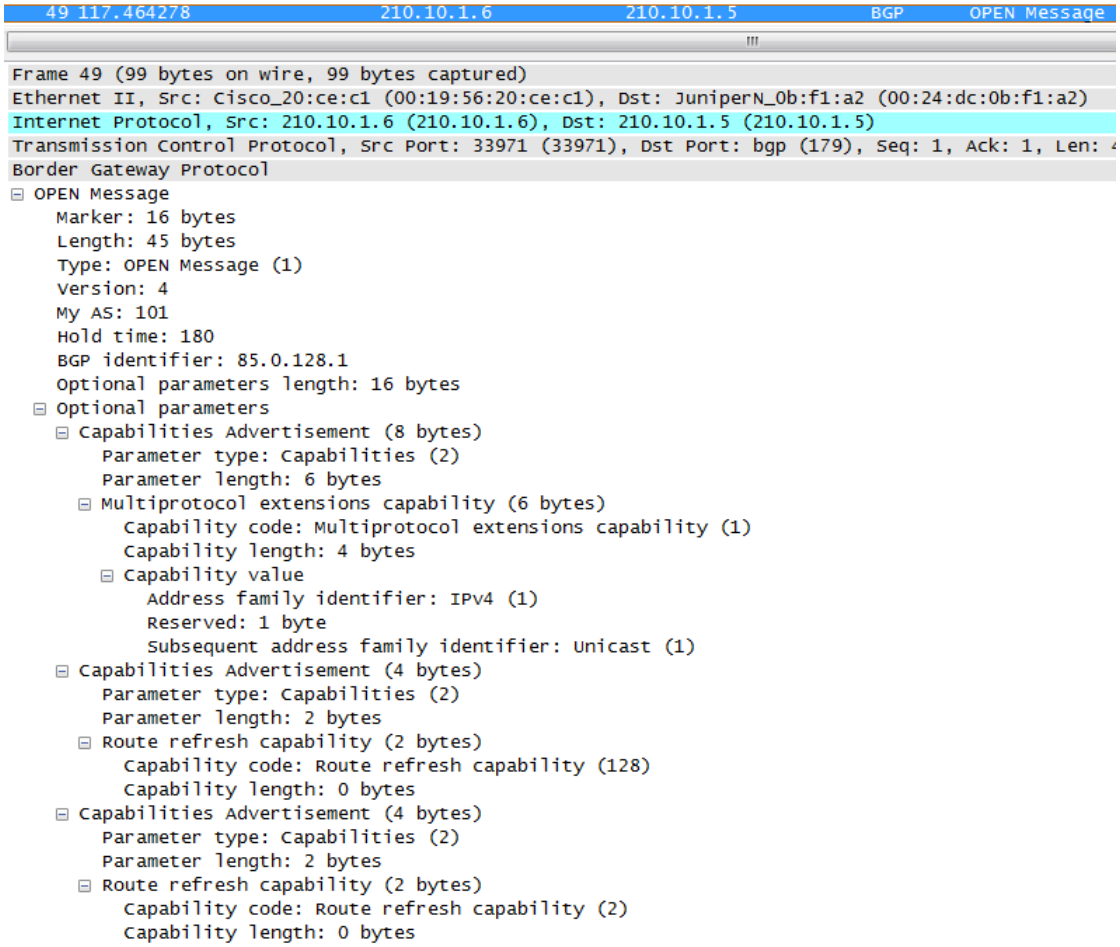


	Time	Source	Destination	Protocol	Info
40	87.194491	210.10.1.5	210.10.1.6	BGP	NOTIFICATION Message
41	87.194494	210.10.1.5	210.10.1.6	TCP	54157 > bgp [FIN, ACK] Seq=79 Ack=58
42	87.196188	210.10.1.6	210.10.1.5	TCP	bgp > 54157 [ACK] Seq=58 Ack=80 Win=1
43	87.200238	210.10.1.6	210.10.1.5	TCP	bgp > 54157 [FIN, PSH, ACK] Seq=58 Ac
44	87.202986	210.10.1.5	210.10.1.6	TCP	54157 > bgp [ACK] Seq=80 Ack=59 Win=1
45	99.349426	Cisco_20:ce:c1	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: Core-R1 Port ID: FastEthe
46	117.458168	210.10.1.6	210.10.1.5	TCP	33971 > bgp [SYN] Seq=0 Win=16384 Ler
47	117.459938	210.10.1.5	210.10.1.6	TCP	bgp > 33971 [SYN, ACK] Seq=0 Ack=1 Wi
48	117.461383	210.10.1.6	210.10.1.5	TCP	33971 > bgp [ACK] Seq=1 Ack=1 Win=163
49	117.464278	210.10.1.6	210.10.1.5	BGP	OPEN Message
50	117.466339	210.10.1.5	210.10.1.6	BGP	OPEN Message
51	117.469581	210.10.1.6	210.10.1.5	BGP	KEEPALIVE Message
52	117.473775	210.10.1.5	210.10.1.6	BGP	KEEPALIVE Message
53	117.481045	210.10.1.6	210.10.1.5	BGP	UPDATE Message, UPDATE Message, UPDAT
54	117.486913	210.10.1.5	210.10.1.6	BGP	KEEPALIVE Message, UPDATE Message, UP
55	117.496593	210.10.1.6	210.10.1.5	BGP	UPDATE Message
56	117.499261	210.10.1.5	210.10.1.6	BGP	UPDATE Message
57	117.502619	210.10.1.6	210.10.1.5	BGP	KEEPALIVE Message, KEEPALIVE Message

KUVIO 66. BGP-yhteyden muodostus

Kuviossa 67 on Wireshark-pakettikaappaus Open-viestistä CiscoCore-R1:ltä Juniper-R5:lle. Open-viestistä on nähtävissä seuraavat tiedot:

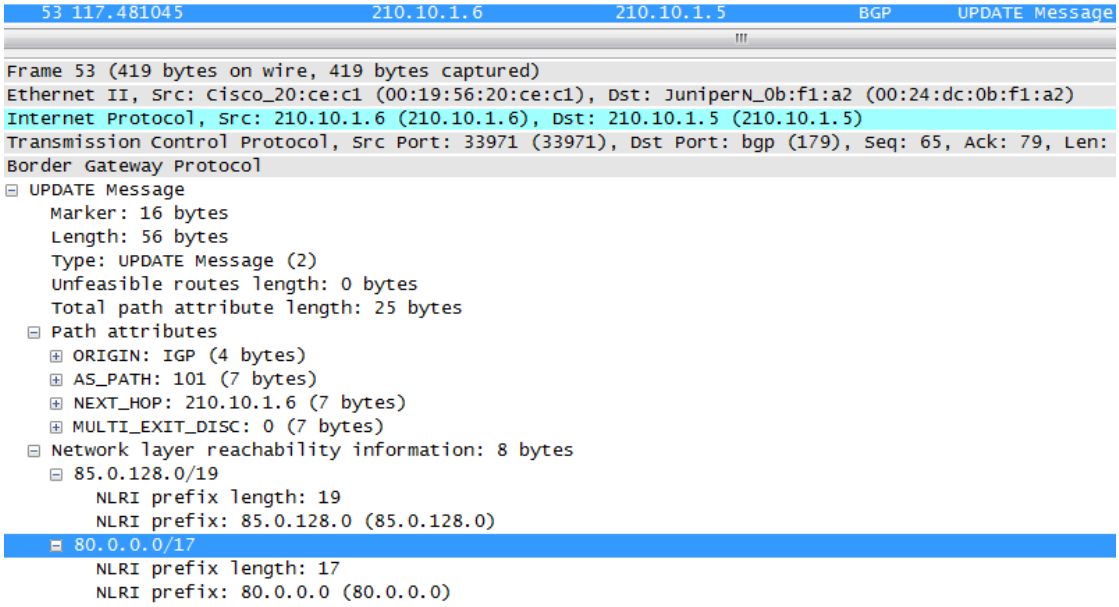
- Viesti tyyppi: *Type: OPEN Message (1)*
- BGP:n versio: *Version: 4*
- Lähettäjän AS-numero: *My AS:101*
- Hold-ajastimen aika: *Hold time: 180*
- BGP-ID: *BGP identifier: 85.0.128.1*
- Sekä joukko kyvykkyysmainoksia (Capabilities Advertisement), joilla BGP-osapuolet neuvottelevat käytettävät BGP-ominaisuudet



KUVIO 67. Wireshark-pakettikaappaus BGP Open -viestistä

Kuviossa 68 on Wireshark-pakettikaappaus BGP Update -viestistä CiscoCore-R1:ltä Juniper-R5:lle. Update-viestissä välitetään seuraavat tiedot:

- Viesti tyyppi: *Type: UPDATE Message (2)*
- Polku-attribuutin pituus: *Total path attributes length: 25 bytes*
- Polku-attribuutit, joissa on seuraavat tiedot:
    - Lähde, josta reitti on opittu: *Origin: IGP*
    - AS-polku, jossa on kaikki AS:t matkalla kyseiseen reittitietoon: *AS_PATH: 101*
    - Seuraavan hypyn IP-osoite: *NEXT_HOP: 210.10.1.6*
    - Multiple Exit Discriminator -attribuutti: *MULTI_EXIT_DISC: 0*
- Reittitieto: *Network layer reachability information: 85.0.128.0/19 ja 80.0.0.0/17*



KUVIO 68. Wireshark-pakettikaappaus BGP Update -viestistä

Kuviossa 69 on kuvankaappaus CiscoCore-R1:n eli AS101-reitittimen IP BGP -reittitaulusta, josta nähdään, että kuviossa 68 olevat reittitiedot ovat CiscoCore-R1:een kytkettyjä verkkoja. Lisäksi nähdään, että Juniper-R5:n mainostamana on opittu 130.100.0.0/16-verkko, joka on siis Juniper-R5:n ja Juniper-R4:n mainostama summaverkko. Summaverkon käyttö estää pienien verkkojen leviämisen ”Internetiin” ja näin osaltaan Operaattori huolehtii siitä, ettei reittitaulut paisu liian suuriksi. Lisäksi todellisuudessa operaattorit eivät tänä päivänä hyväksy /24-verkkoja pienempia aliverkkoja reittimainostuksissa, vaan ne hylätään.

```
Core-R1#show ip bgp
BGP table version is 19, local router ID is 85.0.128.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  12.0.0.0         210.10.1.10                            0 106 102 i
*>                  210.10.1.14              0             0 102 i
*  30.10.0.0/16     210.10.1.14                            0 102 106 105 i
*>                  210.10.1.10                            0 106 105 i
*> 80.0.0.0/17      0.0.0.0                  0         32768 i
*> 85.0.128.0/19    0.0.0.0                  0         32768 i
*  100.80.192.0/18  210.10.1.14                            0 102 106 104 i
*>                  210.10.1.10                            0 106 104 i
*> 130.100.0.0      210.10.1.5                             0 100 i
*                   210.10.1.14                            0 102 103 100 i
*                   210.10.1.10                            0 106 103 100 i
*  150.40.64.0/18   210.10.1.14                            0 102 106 i
*>                  210.10.1.10              0             0 106 i
*  191.145.224.0/19 210.10.1.14                            0 102 106 105 i
*>                  210.10.1.10                            0 106 105 i
*  196.197.208.0/20 210.10.1.14                            0 102 106 i
*>                  210.10.1.10              0             0 106 i
   Network          Next Hop            Metric LocPrf Weight Path
*  200.30.0.0/19    210.10.1.5                             0 100 103 i
*>                  210.10.1.14                            0 102 103 i
*                   210.10.1.10                            0 106 103 i
*  200.35.0.0/21    210.10.1.5                             0 100 103 i
*>                  210.10.1.14                            0 102 103 i
*                   210.10.1.10                            0 106 103 i
```

KUVIO 69. CiscoCore-R1:n IP BGP -reittitaulu

Seuraavana varmistin, että Yritys1:n julkiseen verkkoon on tosiaan pääsy ”Internetistä”. Tämän tein käyttämällä Ping-sovellusta CiscoCore-R6:lla, joka on ns. keskellä ”Internetiä”. Kuviossa 70 on ajettu Ping CiscoCore-R6:n Loopback-rajapinnasta 196.197.208.1/20, joka siis simuloi kyseiseen AS-alueeseen liitettyjä verkkoja, Yritys1:n WG1-SW1-L3-kytkimen julkisen IP-osoitealueen rajapintaan 130.100.10.1.

```
Core-r6#sh ip int bri
Interface                  IP-Address      OK? Method Status                Prot
ocol
GigabitEthernet0/1         210.10.1.10     YES manual up                    up

GigabitEthernet0/2         210.10.1.22     YES manual up                    up

GigabitEthernet0/3         210.10.1.26     YES manual up                    up

FastEthernet1/0            210.10.1.34     YES manual up                    up

FastEthernet1/1            210.10.1.38     YES manual up                    up

ATM2/0                     unassigned      YES manual administratively down down

ATM4/0                     unassigned      YES manual administratively down down

Loopback1                  150.40.64.1     YES manual up                    up

Loopback2                  196.197.208.1   YES manual up                    up

Core-r6#ping 130.100.10.1 source 196.197.208.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 130.100.10.1, timeout is 2 seconds:
Packet sent with a source address of 196.197.208.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

KUVIO 70. CiscoCore-R6:n rajapinnat ja Ping Yritys1:n julkisen verkon reititysrajapintaan

”Internetin” toteuttamisessa sallin kaikkien reittien mainostuksen ympäri ”Internetiä” poislukien Operaattorin 130.100.0.0-verkon pienet aliverkot. Todellisuudessa operaattorien väliset liikennöintisopimukset ratkaisisivat pitkälti, miten reittejä jaetaan ja varsinkin mitä reittejä/AS-alueita suosittaisiin liikenteen välittämisessä Internetiin. Reitityspäätöksiin voidaan vaikuttaa rakentamalla sopivia politiikkoja, joiden perusteella esimerkiksi hyväksyttäisiin vain tietystä AS-alueesta tulevat mainostukset.

10 YHTEENVETO

10.1 Toteutus ja siitä saadut tulokset

Työn toteutus alkoi tutustumalla Juniper-reitittimien toimintaperiaatteisiin ja konfigurointiin, minkä jälkeen verkon konfiguroiminen alkoi. Metro Ethernet -alueiden ja ”Internetin” konfiguroiminen oli suhteellisen helppo vaihe työssä, koska olin jo aikaisemmin tutustunut ja konfiguroinut kyseisille laitteille tarvittavia tekniikoita.

Työn tuloksena syntynyt operaattoritasoinen verkko sekä siihen implementoitu VPLS-palvelu ja sen liitttäminen reititykseen tulee varmasti tukemaan tietoverkkotekniikan

koulutusta laboratorioharjoituksissa ja opetuksessa. Lisäksi BGP-protokollan täysimittainen käyttäminen runkoverkossa lisää opetuksen laajuutta. BGP- ja LDP-protokollien käyttäminen signalointiprotokollina VPN:ien luomiseen myös tuo lisäarvoa koulutukseen.

Tässä opinnäytetyössä suurimmassa käytössä olleet Juniper Networks:n J-series reitittimet antoivat minulle positiivisen kuvan kyseisen laitevalmistajan tuotteista. Juniper-reitittimien käyttäminen on varsin loogista ja tehokasta. Eri tekniikoiden käyttöönotto on mielestäni yksinkertaisempaa kuin muutamien muiden laitevalmistajien tuotteissa. Lisäksi eri VPN:ien tekeminen on erittäin havainnollistavaa konfiguraatioiden osalta, koska niitä ei tehdä reititysprotokollan alle vaan ne ovat omina reititysinstansseinaan.

VPLS-tekniikan oletan yleistyvän verkko-operaattorien käyttöön, koska selkeästi on havaittavissa tarve siirtyä runkoverkoissa pois reitityksestä myös VPN:ien tapauksessa. Nykyisin runkoverkot koostuvat yleisimmin MPLS-tekniikkaan pohjautuvista ratkaisuista, joissa ei liikenteen välityksessä tehdä IP-reittitauluhakuja jokaisella hypyllä vaan ainoastaan kun paketti joko saapuu tai poistuu runkoverkosta. L3-VPN:n tapauksessa tämäkin on turhaa, koska asiakaan sisäisen liikenteen kuljettaminen toimipisteiden välillä vaatii reititystä PE-laitteissa. VPLS tuo ratkaisun tähän ongelmaan, koska siinä liikenteen välitys pohjautuu täysin L2-osoitteisiin ja runkoverkon leimatietoihin. Lisäksi VPLS mahdollistaa E-LAN-palvelun, jossa asiakkaan eri toimipisteet voivat olla loogisesti kytkettynä yhteen yhteiseen lähiverkkoon.

10.2 Pohdinta tulevaisuudesta

Uskon, että VPLS-tekniikka tulee syrjäyttämään MPLS-VPN-ratkaisut tulevaisuudessa operaattorien runkoverkoissa. VPLS:n käyttöönottoa saattaa rajoittaa joidenkin PE-laitteiden riittämätön tuki VPLS:lle, mistä seuraa, että VPLS ja MPLS-VPN tulevat olemaan käytössä rinnakkain varsin pitkään. VPLS-toteutuksia on jo maailmalla käytössä ainakin Verizon verkko-operaattorilla Yhdysvaltojen alueella ja varmasti muillakin verkko-operaattoreilla.

Opinnäytteessäni olleet ongelmat J-series-reitittimien kanssa pitäisi Juniper:lta saadun tiedon mukaan korjaantua JUNOS-käyttöjärjestelmän päivityksessä vuoden 2010 ai-

kana. Päivityksen yhteydessä lisättävä Stacked-VLAN-Tagging-ominaisuus mahdollistaa lenkkikaapeliratkaisun hylkäämisen ja asiakkuuden reititykseen viemisen tekemisen ”oikealla” tavalla heti Metro Ethernet -alueeseen liittyvässä rajapinnassa.

L2-Circuit olisi varmasti hyvä tutkimuksen kohde opinnäytteeni jatkokehitykselle. L2-Circuit:eilla on mahdollista luoda valmiita tunneleita PE-laitteiden välille, jolloin VPLS-signalointiprotokollien ei tarvitse jokaiselle VPLS-instanssille luoda omia virtuaalilinkkejä vaan VPLS-instanssien liikenne voitaisiin kuljettaa L2-Circuit:eja pitkin PE-laitteiden välillä.

LÄHTEET

Andersson, L., Minei, I. & Thomas, B. 2007. RFC 5036 LDP Specification. Internet RFC Archives.

Bates, T., Chandra, R. & Chen, E. 2006. RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP). Internet RFC Archives.

Callon, R., Rosen, E. & Viswanathan, A. 2001. RFC 3031 Multiprotocol Label Switching Architecture. Internet RFC Archives.

Conta, A., Farinacci, D., Fedorkow, G., Li, T., Rekhter, Y., Rosen, E. & Tappan, D. 2001. RFC 3032 MPLS Label Stack Encoding. Internet RFC Archives.

De Clercq, J., Khandekar, S. & Witters, J. 2009. VPLS technical tutorial. Viitattu 12.9.2009. Alcatel-Lucent.

DeHaven Carroll, J. & Doyle, J. 2001. CCIE Professional Development Routing TCP/IP Volume II. Indianapolis. Cisco Press.

Guichard, J. & Pepelnjak, I. 2001. MPLS and VPN Architectures. Indianapolis. Cisco Press.

El-Aawar, N., Heron, G., Martini, L., Rosen, E. & Smith, T. 2006. RFC 4447 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP). Internet RFC Archives.

Extreme Networks. 2009. ExtremeXOS Concepts Guide Software Version 12.1. Viitattu 5.9.2009.

Hares, S., Li, T. & Rekhter, Y. 2006. RFC 4271 Border Gateway Protocol 4 (BGP-4). RFC Internet Archives.

Juniper Networks. 2009a. Juniper Networksin historia. Viitattu 26.8.2009. Http:// http://www.juniper.net/us/en/local/pdf/fact-sheets-backgrounder/3000054-en.pdf

Juniper Networks. 2009b. Juniper Networksin laitteet. Viitattu 27.8.2009. Http:// http://www.juniper.net/us/en/products-services

Juniper Networks. 2009c. JUNOS Software: The Power of One Operating System. Viitattu 29.8.2009. Http://www.juniper.net/us/en/local/pdf/app-notes/3500145-en.pdf

Juniper Networks. 2009d. Virtual Private LAN Service White Paper. Viitattu 12.9.2009. Http://www.juniper.net/solutions/literature/white_papers/200045.pdf

Jyväskylän ammattikorkeakoulu. 2009. Tutustu JAMKiin. Viitattu 16.8.2009. Http://www.jamk.fi, tutustu.

Kompella, K. & Lasserre, M. 2007. RFC 4762 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling. Internet RFC Archives.

Kompella, K. & Rekhter, Y. 2007. RFC 4761 Virtual Private LAN Service (VPLS) using BGP for Auto-Discovery and Signaling. Internet RFC Archives.

Lynch, L. & Solie, K. 2003. CCIE practical studies. Indianapolis. Cisco Press.

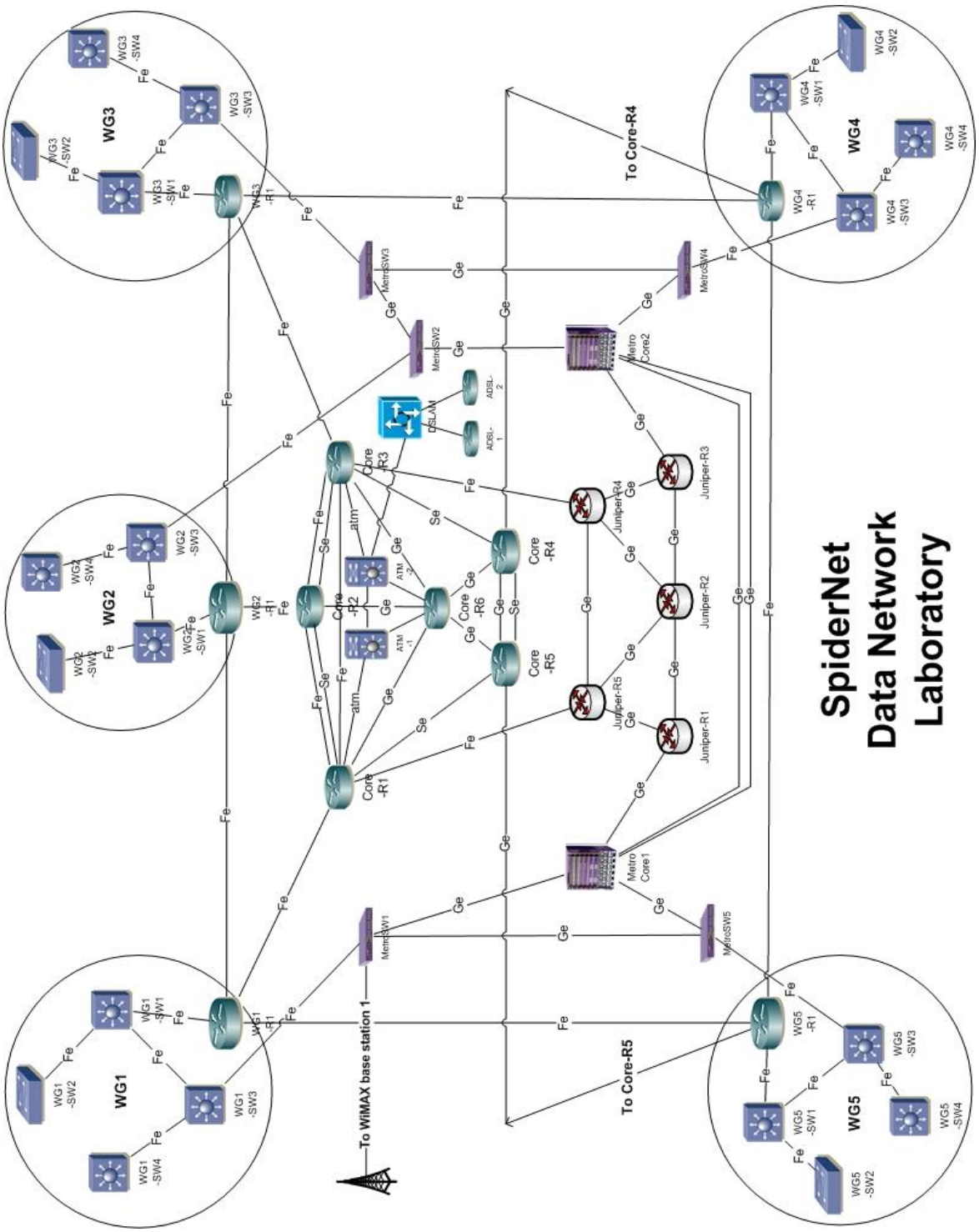
Marschke, D. & Reynolds, H. 2008. JUNOS Enterprise Routing. Sebastopol. O'Reilly.

Metro Ethernet Forum. 2009a. Metro Ethernet Networks – A Techical Overview. Viitattu 5.9.2009. Http://metroethernetforum.org/PDF_Documents/metro-ethernet-networks.pdf

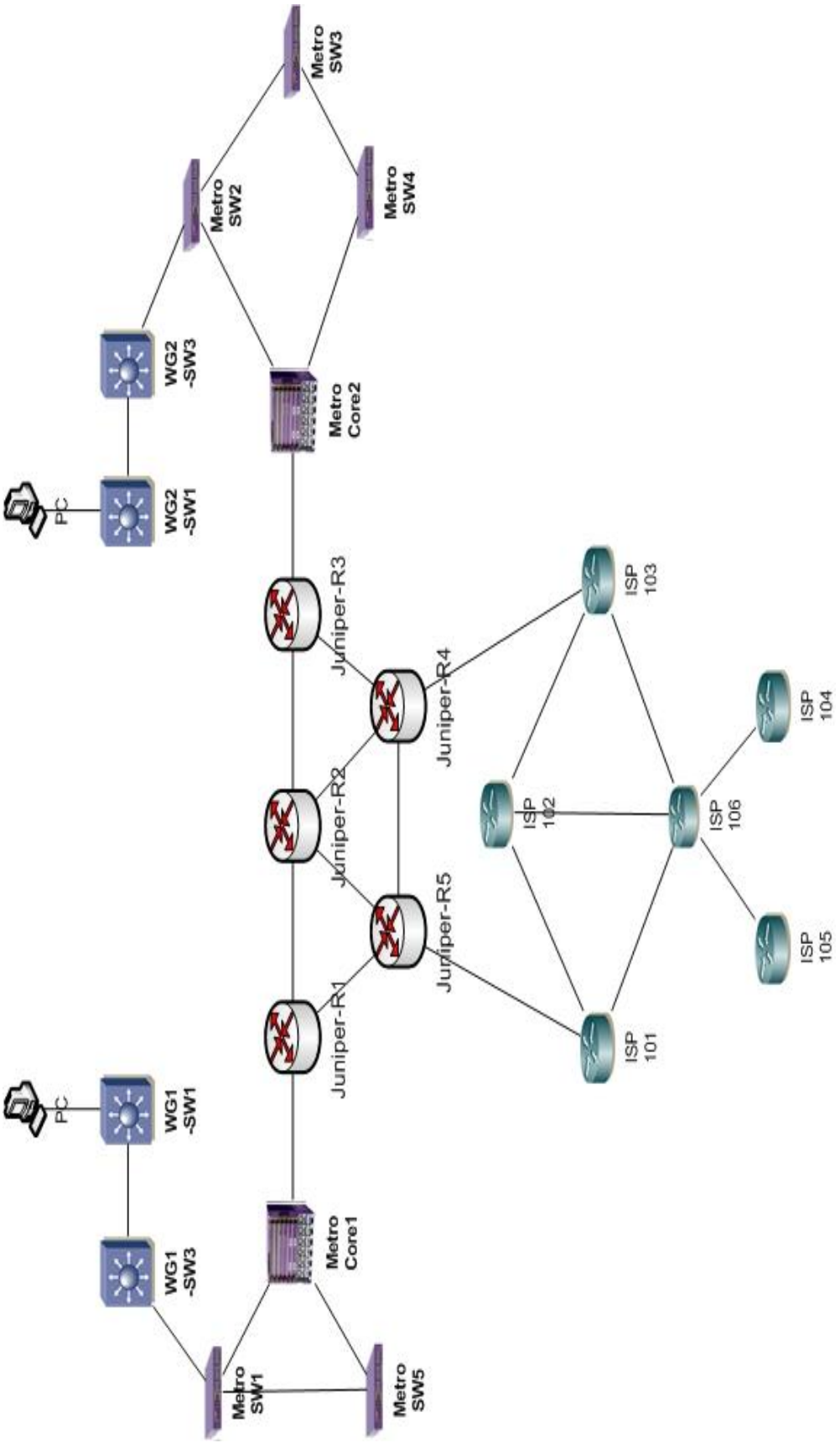
Metro Ethernet Forum. 2009b. Metro Ethernet Services – A Technical Overview. Viitattu 5.9.2009. Http://metroethernetforum.org/PDF_Documents/metro-ethernet-services.pdf

LIITTEET

Liite 1. SpiderNet-topologia



Liite 2. Verkon topologia



Liite 3. Juniper-R1-konfiguraatiot, VPLS BGP-signaloituna

```
root@Juniper-R1# show
## Last changed: 2009-10-21 21:04:01 UTC
version 9.6R1.13;
system {
    host-name Juniper-R1;
    root-authentication {
        encrypted-password "$1$a2zNuu5v$J5q27U5ZblDo6kguolWuy."; ## SECRET-DATA
    }
    services {
        ssh;
        web-management {
            http {
                interface ge-0/0/0.0;
            }
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any any;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
chassis {
    fpc 1 {
        pic 0 {
            ethernet {
                pic-mode routing;
            }
        }
    }
}
interfaces {
    ge-0/0/1 {
        unit 0;
    }
    ge-0/0/2 {
        unit 0;
    }
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 10.0.0.1/24;
            }
            family mpls;
```

```
        }
    }
    ge-1/0/1 {
        unit 0 {
            family inet {
                address 10.0.4.1/24;
            }
            family mpls;
        }
    }
    ge-1/0/2 {
        vlan-tagging;
        encapsulation extended-vlan-vpls;
        unit 101 {
            vlan-id 512;
            family vpls;
        }
    }
    ge-1/0/3 {
        vlan-tagging;
        encapsulation vlan-vpls;
        unit 101 {
            encapsulation vlan-vpls;
            vlan-id 1001;
            input-vlan-map {
                push;
                vlan-id 512;
            }
            output-vlan-map pop;
            family vpls;
        }
    }
    ge-1/0/4 {
        vlan-tagging;
        unit 101 {
            vlan-id 1001;
            family inet {
                address 130.100.8.1/30;
            }
        }
    }
    ge-1/0/5 {
        unit 0;
    }
    ge-1/0/6 {
        unit 0;
    }
    ge-1/0/7 {
        unit 0;
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.1/32;
            }
        }
    }
}
routing-options {
    static {
```

```
        route 130.100.10.0/24 next-hop 130.100.8.2;
    }
    router-id 172.16.1.1;
    autonomous-system 100;
}
protocols {
    mpls {
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
    }
    bgp {
        group VPLS_BGP {
            type internal;
            description "iBGP for VPLS";
            local-address 172.16.1.1;
            family l2vpn {
                signaling;
            }
            neighbor 172.16.1.3;
        }
        group Inter_BGP {
            type internal;
            local-address 172.16.1.1;
            export [ static_to_bgp connected_to_bgp ];
            neighbor 172.16.1.4;
            neighbor 172.16.1.5;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface ge-1/0/0.0;
            interface ge-1/0/1.0;
            interface lo0.0;
        }
    }
    ldp {
        keepalive-interval 10;
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
    }
}
policy-options {
    policy-statement connected_to_bgp {
        from {
            protocol direct;
            route-filter 130.100.0.0/16 orlonger;
        }
        then accept;
    }
    policy-statement static_to_bgp {
        term 1 {
            from protocol static;
            then accept;
        }
    }
}
security {
    forwarding-options {
        family {
            mpls {
```

```
            mode packet-based;
        }
    }
  }
}
routing-instances {
  Yritys1_VPLS {
    instance-type vpls;
    interface ge-1/0/2.101;
    interface ge-1/0/3.101;
    route-distinguisher 100:101;
    vrf-target target:100:101;
    protocols {
      vpls {
        site-range 20;
        no-tunnel-services;
        site Yritys1_WG1 {
          site-identifier 1;
          interface ge-1/0/2.101 {
            interface-mac-limit {
              20000;
            }
          }
        }
      }
    }
  }
}
```

Liite 4. Juniper-R1-konfiguraatiot, VPLS LDP-signaloituna

```
root@Juniper-R1# show
## Last changed: 2009-10-22 00:14:30 UTC
version 9.6R1.13;
system {
  host-name Juniper-R1;
  root-authentication {
    encrypted-password "$1$a2zNuu5v$J5q27U5ZblDo6kguolWuy."; ## SECRET-DATA
  }
  services {
    ssh;
    web-management {
      http {
        interface ge-0/0/0.0;
      }
    }
  }
  syslog {
    user * {
      any emergency;
    }
    file messages {
      any any;
      authorization info;
    }
    file interactive-commands {
      interactive-commands any;
```

```
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
chassis {
    fpc 1 {
        pic 0 {
            ethernet {
                pic-mode routing;
            }
        }
    }
}
interfaces {
    ge-0/0/1 {
        unit 0;
    }
    ge-0/0/2 {
        unit 0;
    }
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 10.0.0.1/24;
            }
            family mpls;
        }
    }
    ge-1/0/1 {
        unit 0 {
            family inet {
                address 10.0.4.1/24;
            }
            family mpls;
        }
    }
    ge-1/0/2 {
        vlan-tagging;
        encapsulation extended-vlan-vpls;
        unit 101 {
            vlan-id 512;
            family vpls;
        }
    }
    ge-1/0/3 {
        vlan-tagging;
        encapsulation vlan-vpls;
        unit 101 {
            encapsulation vlan-vpls;
            vlan-id 1001;
            input-vlan-map {
                push;
                vlan-id 512;
            }
            output-vlan-map pop;
            family vpls;
```

```
        }
    }
    ge-1/0/4 {
        vlan-tagging;
        unit 101 {
            vlan-id 1001;
            family inet {
                address 130.100.8.1/30;
            }
        }
    }
    ge-1/0/5 {
        unit 0;
    }
    ge-1/0/6 {
        unit 0;
    }
    ge-1/0/7 {
        unit 0;
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.1/32;
            }
        }
    }
}
routing-options {
    static {
        route 130.100.10.0/24 next-hop 130.100.8.2;
    }
    router-id 172.16.1.1;
    autonomous-system 100;
}
protocols {
    mpls {
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
    }
    bgp {
        group Inter_BGP {
            type internal;
            local-address 172.16.1.1;
            export [ static_to_bgp connected_to_bgp ];
            neighbor 172.16.1.4;
            neighbor 172.16.1.5;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface ge-1/0/0.0;
            interface ge-1/0/1.0;
            interface lo0.0;
        }
    }
    ldp {
        keepalive-interval 10;
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
```

```
        interface lo0.0;
    }
}
policy-options {
    policy-statement connected_to_bgp {
        from {
            protocol direct;
            route-filter 130.100.0.0/16 orlonger;
        }
        then accept;
    }
    policy-statement static_to_bgp {
        term 1 {
            from protocol static;
            then accept;
        }
    }
}
security {
    forwarding-options {
        family {
            mpls {
                mode packet-based;
            }
        }
    }
}
routing-instances {
    Yritys1_VPLS {
        instance-type vpls;
        interface ge-1/0/2.101;
        interface ge-1/0/3.101;
        protocols {
            vpls {
                no-tunnel-services;
                vpls-id 10;
                neighbor 172.16.1.3;
                connectivity-type ce;
            }
        }
    }
}
```

Liite 5. Juniper-R2-konfiguraatiot

```
root@Juniper-R2# show
## Last changed: 2009-10-07 21:02:38 UTC
version 9.5R1.8;
system {
    host-name Juniper-R2;
    root-authentication {
        encrypted-password "$1$a2zNuu5v$J5q27U5ZblDo6kguolWuy."; ## SECRET-DATA
    }
    services {
        ssh;
        web-management {
            http {
```

```
            interface ge-0/0/0.0;
        }
    }
}
syslog {
    user * {
        any emergency;
    }
    file messages {
        any any;
        authorization info;
    }
    file interactive-commands {
        interactive-commands any;
    }
}
license {
    autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
    }
}
}
interfaces {
    ge-0/0/0 {
        unit 0;
    }
    ge-0/0/1 {
        unit 0;
    }
    ge-0/0/2 {
        unit 0;
    }
    ge-0/0/3 {
        unit 0;
    }
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 10.0.1.1/24;
            }
            family mpls;
        }
    }
    ge-1/0/1 {
        unit 0 {
            family inet {
                sampling {
                    input;
                }
                address 10.0.0.2/24;
            }
            family mpls;
        }
    }
    ge-1/0/2 {
        unit 0 {
            family inet {
                address 10.0.6.1/24;
            }
            family mpls;
```

```
        }
    }
    ge-1/0/3 {
        unit 0 {
            family inet {
                address 10.0.5.1/24;
            }
            family mpls;
        }
    }
    ge-1/0/4 {
        unit 0;
    }
    ge-1/0/5 {
        unit 0;
    }
    ge-1/0/6 {
        unit 0;
    }
    ge-1/0/7 {
        unit 0;
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.2/32;
            }
        }
    }
}
protocols {
    mpls {
        interface ge-1/0/1.0;
        interface ge-1/0/3.0;
        interface ge-1/0/0.0;
        interface ge-1/0/2.0;
    }
    ospf {
        area 0.0.0.0 {
            interface ge-1/0/1.0;
            interface ge-1/0/0.0;
            interface ge-1/0/3.0;
            interface ge-1/0/2.0;
            interface lo0.0;
        }
    }
    ldp {
        keepalive-interval 10;
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
        interface ge-1/0/2.0;
        interface ge-1/0/3.0;
    }
}
security {
    forwarding-options {
        family {
            mpls {
                mode packet-based;
            }
```

```
        }
    }
}
```

Liite 6. Juniper-R3-konfiguraatiot, VPLS BGP-signaloituna

```
root@Juniper-R3# show
## Last changed: 2009-10-07 22:00:06 UTC
version 9.5R1.8;
system {
    host-name Juniper-R3;
    root-authentication {
        encrypted-password "$1$a2zNuu5v$J5q27U5ZblDo6kguolWuy."; ## SECRET-DATA
    }
    services {
        ssh;
        web-management {
            http {
                interface ge-0/0/0.0;
            }
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any any;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
chassis {
    fpc 1 {
        pic 0 {
            ethernet {
                pic-mode routing;
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0;
    }
    ge-0/0/1 {
        unit 0;
    }
    ge-0/0/2 {
```

```
        unit 0;
    }
    ge-0/0/3 {
        unit 0;
    }
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 10.0.2.1/24;
            }
            family mpls;
        }
    }
    ge-1/0/1 {
        unit 0 {
            family inet {
                address 10.0.1.2/24;
            }
            family mpls;
        }
    }
    ge-1/0/2 {
        vlan-tagging;
        encapsulation extended-vlan-vpls;
        unit 101 {
            vlan-id 512;
            family vpls;
        }
    }
    ge-1/0/3 {
        unit 0;
    }
    ge-1/0/4 {
        unit 0;
    }
    ge-1/0/5 {
        unit 0;
    }
    ge-1/0/6 {
        unit 0;
    }
    ge-1/0/7 {
        unit 0;
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.3/32;
            }
        }
    }
}
routing-options {
    router-id 172.16.1.3;
    autonomous-system 100;
}
protocols {
    mpls {
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
```

```
    }
    bgp {
        group VPLS_BGP {
            type internal;
            description "iBGP for VPLS";
            local-address 172.16.1.3;
            family l2vpn {
                signaling;
            }
            neighbor 172.16.1.1;
        }
        group Inter_BGP {
            type internal;
            local-address 172.16.1.3;
            neighbor 172.16.1.5;
            neighbor 172.16.1.4;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface ge-1/0/1.0;
            interface ge-1/0/0.0;
            interface lo0.0;
        }
    }
    ldp {
        keepalive-interval 10;
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
    }
}
security {
    forwarding-options {
        family {
            mpls {
                mode packet-based;
            }
        }
    }
}
routing-instances {
    Yritys1_VPLS {
        instance-type vpls;
        interface ge-1/0/2.101;
        route-distinguisher 100:101;
        vrf-target target:100:101;
        protocols {
            vpls {
                site-range 20;
                no-tunnel-services;
                site Yritys1_WG2 {
                    site-identifier 2;
                    interface ge-1/0/2.101;
                }
            }
        }
    }
}
```

Liite 7. Juniper-R3-konfiguraatiot, VPLS LDP-signaloituna

```
root@Juniper-R3# show
## Last changed: 2009-10-22 00:10:55 UTC
version 9.5R1.8;
system {
    host-name Juniper-R3;
    root-authentication {
        encrypted-password "$1$a2zNuu5v$J5q27U5ZblDo6kguolWuy."; ## SECRET-DATA
    }
    services {
        ssh;
        web-management {
            http {
                interface ge-0/0/0.0;
            }
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any any;
            authorization info;
        }


        file interactive-commands {
            interactive-commands any;
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
chassis {
    fpc 1 {
        pic 0 {
            ethernet {
                pic-mode routing;
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0;
    }
    ge-0/0/1 {
        unit 0;
    }
    ge-0/0/2 {
        unit 0;
    }
    ge-0/0/3 {
```

```
        unit 0;
    }
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 10.0.2.1/24;
            }
            family mpls;
        }
    }
    ge-1/0/1 {
        unit 0 {
            family inet {
                address 10.0.1.2/24;
            }
            family mpls;
        }
    }
    ge-1/0/2 {
        vlan-tagging;
        encapsulation extended-vlan-vpls;
        unit 101 {
            vlan-id 512;
            family vpls;
        }
    }
    ge-1/0/3 {
        unit 0;
    }
    ge-1/0/4 {
        unit 0;
    }
    ge-1/0/5 {
        unit 0;
    }
    ge-1/0/6 {
        unit 0;
    }
    ge-1/0/7 {
        unit 0;
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.3/32;
            }
        }
    }
}
routing-options {
    router-id 172.16.1.3;
    autonomous-system 100;
}
protocols {
    mpls {
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
    }
    bgp {
        group Inter_BGP {
```

```
            type internal;
            local-address 172.16.1.3;
            neighbor 172.16.1.5;
            neighbor 172.16.1.4;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface ge-1/0/1.0;
            interface ge-1/0/0.0;
            interface lo0.0;
        }
    }
    ldp {
        keepalive-interval 10;
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
        interface lo0.0;
    }
}
security {
    forwarding-options {
        family {
            mpls {
                mode packet-based;
            }
        }
    }
}
routing-instances {
    Yritys1_VPLS {
        instance-type vpls;
        interface ge-1/0/2.101;
        protocols {
            vpls {
                no-tunnel-services;
                vpls-id 10;
                neighbor 172.16.1.1;
                connectivity-type ce;
            }
        }
    }
}
```

Liite 8. Juniper-R4-konfiguraatiot

```
root@Juniper-R4# show
## Last changed: 2009-10-21 21:43:04 UTC
version 9.5R1.8;
system {
    host-name Juniper-R4;
    root-authentication {
        encrypted-password "$1$a2zNuu5v$J5q27U5ZblDo6kguolWuy."; ## SECRET-DATA
    }
    services {
        ssh;
        web-management {
```

```
            http {
                interface ge-0/0/0.0;
            }
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any any;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0;
    }
    ge-0/0/1 {
        unit 0;
    }
    ge-0/0/2 {
        unit 0;
    }
    ge-0/0/3 {
        unit 0;
    }
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 10.0.3.1/24;
            }
            family mpls;
        }
    }
    ge-1/0/1 {
        unit 0 {
            family inet {
                address 10.0.2.2/24;
            }
            family mpls;
        }
    }
    ge-1/0/2 {
        unit 0 {
            family inet {
                address 210.10.1.1/30;
            }
        }
    }
    ge-1/0/3 {
```

```
        disable;
        unit 0 {
            family inet {
                address 10.0.6.2/24;
            }
            family mpls;
        }
    }
    ge-1/0/4 {
        unit 0;
    }
    ge-1/0/5 {
        unit 0;
    }
    ge-1/0/6 {
        unit 0;
    }
    ge-1/0/7 {
        unit 0;
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.4/32;
            }
        }
    }
}
routing-options {
    aggregate {
        route 130.100.0.0/16;
    }
    router-id 172.16.1.4;
    autonomous-system 100;
}
protocols {
    mpls {
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
        interface ge-1/0/3.0;
    }
    bgp {
        group Inter_BGP {
            type internal;
            local-address 172.16.1.4;
            export external_import;
            cluster 1.2.3.4;
            neighbor 172.16.1.5;
            neighbor 172.16.1.1;
            neighbor 172.16.1.3;
        }
        group AS_103 {
            type external;
            local-address 210.10.1.1;
            export advertise_only_aggregate;
            peer-as 103;
            neighbor 210.10.1.2;
        }
    }
    ospf {
```

```
        area 0.0.0.0 {
            interface ge-1/0/1.0;
            interface ge-1/0/0.0;
            interface ge-1/0/3.0;
            interface lo0.0;
        }
    }
    ldp {
        keepalive-interval 10;
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
        interface ge-1/0/3.0;
    }
}
policy-options {
    policy-statement advertise_only_aggregate {
        term 1 {
            from protocol aggregate;
            then accept;
        }
        term 2 {
            from {
                protocol bgp;
                route-filter 130.100.0.0/16 longer;
            }
            then reject;
        }
    }
    policy-statement external_import {
        term 1 {
            from protocol bgp;
            then {
                next-hop self;
                accept;
            }
        }
        term 2 {
            then reject;
        }
    }
}
security {
    forwarding-options {
        family {
            mpls {
                mode packet-based;
            }
        }
    }
}
```

Liite 9. Juniper-R5-konfiguraatiot

```
root@Juniper-R5# show
## Last changed: 2009-10-21 21:44:50 UTC
version 9.5R1.8;
system {
```

```
    host-name Juniper-R5;
    root-authentication {
        encrypted-password "$1$a2zNuu5v$J5q27U5ZblDo6kguolWuy."; ## SECRET-DATA
    }
    services {
        ssh;
        web-management {
            http {
                interface ge-0/0/0.0;
            }
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any any;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
    license {
        autoupdate {
            url https://ae1.juniper.net/junos/key_retrieval;
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0;
    }
    ge-0/0/1 {
        unit 0;
    }
    ge-0/0/2 {
        unit 0;
    }
    ge-0/0/3 {
        unit 0;
    }
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 10.0.4.2/24;
            }
            family mpls;
        }
    }
    ge-1/0/1 {
        unit 0 {
            family inet {
                address 10.0.3.2/24;
            }
            family mpls;
        }
    }
    ge-1/0/2 {
```

```
        unit 0 {
            family inet {
                address 210.10.1.5/30;
            }
        }
    }
    ge-1/0/3 {
        unit 0 {
            family inet {
                address 10.0.5.2/24;
            }
            family mpls;
        }
    }
    ge-1/0/4 {
        unit 0;
    }
    ge-1/0/5 {
        unit 0;
    }
    ge-1/0/6 {
        unit 0;
    }
    ge-1/0/7 {
        unit 0;
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.5/32;
            }
        }
    }
}
routing-options {
    aggregate {
        route 130.100.0.0/16;
    }
    autonomous-system 100;
}
protocols {
    mpls {
        interface ge-1/0/0.0;
        interface ge-1/0/3.0;
        interface ge-1/0/1.0;
    }
    bgp {
        group Inter_BGP {
            type internal;
            local-address 172.16.1.5;
            export external_import;
            cluster 1.2.3.4;
            neighbor 172.16.1.4;
            neighbor 172.16.1.1;
            neighbor 172.16.1.3;
        }
        group AS_101 {
            type external;
            local-address 210.10.1.5;
            export advertise_only_aggregate;
```

```
            peer-as 101;
            neighbor 210.10.1.6;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface ge-1/0/1.0;
            interface ge-1/0/0.0;
            interface ge-1/0/3.0;
            interface lo0.0;
        }
    }
    ldp {
        keepalive-interval 10;
        interface ge-1/0/0.0;
        interface ge-1/0/1.0;
        interface ge-1/0/3.0;
    }
}
policy-options {
    policy-statement advertise_only_aggregate {
        term 1 {
            from protocol aggregate;
            then accept;
        }
        term 2 {
            from {
                protocol bgp;
                route-filter 130.100.0.0/16 longer;
            }
            then reject;
        }
    }
    policy-statement external_import {
        term 1 {
            from protocol bgp;
            then {
                next-hop self;
                accept;
            }
        }
        term 2 {
            then reject;
        }
    }
}
security {
    forwarding-options {
        family {
            mpls {
                mode packet-based;
            }
        }
    }
}
```

Liite 10. MetroCore1-konfiguraatiot

MCore1.1 # show configuration

Module devmgr configuration.
configure snmp sysName "MCore1"
configure slot 1 module GM-20XTR
configure sys-recovery-level slot 1 reset

Module vlan configuration.
configure vr VR-Default add ports 1:1-20
configure vlan default delete ports 1:1-20
configure vman ethertype 0x8100 primary
create vman "yritys1"
configure vman yritys1 tag 512
create vman "ME_area1_control"
configure vman ME_area1_control tag 1001
configure vman yritys1 add ports 1:3-5 tagged
configure vman ME_area1_control add ports 1:3-4 tagged

Module eaps configuration.
enable eaps
create eaps ME_area1
configure eaps ME_area1 mode master
configure eaps ME_area1 primary port 1:3
configure eaps ME_area1 secondary port 1:4
enable eaps ME_area1
configure eaps ME_area1 add control vlan ME_area1_control
configure eaps ME_area1 add protected vlan yritys1

Liite 11. MetroCore2-konfiguraatiot

Mcore2.1 # show configuration
Module devmgr configuration.
configure snmp sysName "Mcore2"
configure slot 1 module GM-20XTR
configure sys-recovery-level slot 1 reset

Module vlan configuration.
configure vr VR-Default add ports 1:1-20
configure vlan default delete ports 1:1-20
configure vman ethertype 0x8100 primary
create vman "yritys1"
configure vman yritys1 tag 512
create vman "ME_area2_control"
configure vman ME_area2_control tag 1002
configure vman yritys1 add ports 1:3-5 tagged
configure vman ME_area2_control add ports 1:3-4 tagged

Module eaps configuration.
enable eaps
create eaps ME_area2
configure eaps ME_area2 mode master
configure eaps ME_area2 primary port 1:3
configure eaps ME_area2 secondary port 1:4

```
enable eaps ME_area2
configure eaps ME_area2 add control vlan ME_area2_control
configure eaps ME_area2 add protected vlan yritys1
```

Liite 12. MetroSW1-konfiguraatiot

```
* MSW1.2 # sh conf
# Module devmgr configuration.
configure snmp sysName "MSW1"
configure sys-recovery-level switch reset

# Module vlan configuration.
configure vlan default delete ports 1-26
configure vman ethertype 0x8100
create vman "yritys1"
configure vman yritys1 tag 512
configure vman ME_area1_control tag 1001
enable vMan ports 1
configure vman yritys 1 add ports 25-26 tagged
configure vman yritys 1 add ports 1 untagged
configure vman ME_area1_control add ports 25-26 tagged

# Module eaps configuration.
enable eaps
create eaps ME_area1
configure eaps ME_area1 mode transit
configure eaps ME_area1 primary port 25
configure eaps ME_area1 secondary port 26
enable eaps ME_area1
configure eaps ME_area1 add control vlan ME_area1_control
configure eaps ME_area1 add protected vlan yritys1
```

Liite 13. MetroSW2-konfiguraatiot

```
MSW2.1 # sh conf
# Module devmgr configuration.
configure snmp sysName "MSW2"
configure sys-recovery-level switch reset

# Module vlan configuration.
configure vlan default delete ports 1-26
configure vman ethertype 0x8100
create vman "yritys1"
configure vman yritys1 tag 512
create vman "ME_area2_control"
configure vman ME_area2_control tag 1002
enable vMan ports 1
configure vman yritys 1 add ports 25-26 tagged
configure vman yritys 1 add ports 1 untagged
configure vman ME_area2_control add ports 25-26 tagged

# Module eaps configuration.
enable eaps
create eaps ME_area2
```

```
configure eaps ME_area2 mode transit
configure eaps ME_area2 primary port 25
configure eaps ME_area2 secondary port 26
enable eaps ME_area2
configure eaps ME_area2 add control vlan ME_area2_control
configure eaps ME_area2 add protected vlan yritys 1
```

Liite 14. MetroSW3-konfiguraatiot

```
MSW3.1 # show configuration
# Module devmgr configuration.
configure snmp sysName "MSW3"
configure sys-recovery-level switch reset

# Module vlan configuration.
configure vlan default delete ports 1-26
configure vman ethertype 0x8100
create vman " yritys 1"
configure vman yritys 1 tag 512
create vman "ME_area2_control"
configure vman ME_area2_control tag 1002
enable vMan ports 1
configure vman yritys 1 add ports 25-26 tagged
configure vman ME_area2_control add ports 25-26 tagged

# Module eaps configuration.
enable eaps
create eaps ME_area2
configure eaps ME_area2 mode transit
configure eaps ME_area2 primary port 25
configure eaps ME_area2 secondary port 26
enable eaps ME_area2
configure eaps ME_area2 add control vlan ME_area2_control
configure eaps ME_area2 add protected vlan yritys 1
```

Liite 15. MetroSW4-konfiguraatiot

```
MSW4.1 # show configuration
# Module devmgr configuration.
configure snmp sysName "MSW4"
configure sys-recovery-level switch reset

# Module vlan configuration.
configure vlan default delete ports 1-26
configure vman ethertype 0x8100
create vman " yritys 1"
configure vman yritys1 tag 512
create vman "ME_area2_control"
configure vman ME_area2_control tag 1002
enable vMan ports 1
configure vman yritys 1 add ports 25-26 tagged
configure vman ME_area2_control add ports 25-26 tagged

# Module eaps configuration.
```

```
enable eaps
create eaps ME_area2
configure eaps ME_area2 mode transit
configure eaps ME_area2 primary port 25
configure eaps ME_area2 secondary port 26
enable eaps ME_area2
configure eaps ME_area2 add control vlan ME_area2_control
configure eaps ME_area2 add protected vlan yritys 1
```

Liite 16. MetroSW5-konfiguraatiot

```
MSW5.1 # show configuration
# Module devmgr configuration.
configure snmp sysName "MSW5"
configure sys-recovery-level switch reset

# Module vlan configuration.
configure vlan default delete ports 1-26
configure vman ethertype 0x8100
create vman " yritys 1"
configure vman yritys 1 tag 512
create vman "ME_area1_control"
configure vman ME_area1_control tag 1001
enable vMan ports 1
configure vman yritys 1 add ports 25-26 tagged
configure vman ME_area1_control add ports 25-26 tagged

# Module eaps configuration.
enable eaps
create eaps ME_area1
configure eaps ME_area1 mode transit
configure eaps ME_area1 primary port 25
configure eaps ME_area1 secondary port 26
enable eaps ME_area1
configure eaps ME_area1 add control vlan ME_area1_control
configure eaps ME_area1 add protected vlan yritys 1
```

Liite 17. CiscoCore-R1-konfiguraatiot

```
Core-R1#sh run
Current configuration : 1992 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Core-R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 25
```

```
!
ip cef
!
interface Loopback1
 ip address 80.0.0.1 255.255.128.0
!
interface Loopback2
 ip address 85.0.128.1 255.255.224.0
!
interface FastEthernet3/0
 no switchport
 ip address 210.10.1.13 255.255.255.252
!
interface FastEthernet3/3
 description Link to Juniper-R5, port Ge-1/0/2
 no switchport
 ip address 210.10.1.6 255.255.255.252
!
interface GigabitEthernet3/0
 no switchport
 ip address 210.10.1.9 255.255.255.252
!
interface Vlan1
 no ip address
!
router bgp 101
 no synchronization
 bgp log-neighbor-changes
 network 80.0.0.0 mask 255.255.128.0
 network 85.0.128.0 mask 255.255.224.0
 neighbor 210.10.1.5 remote-as 100
 neighbor 210.10.1.10 remote-as 106
 neighbor 210.10.1.14 remote-as 102
 no auto-summary
!
ip http server
no ip http secure-server
!
end
```

Liite 18. CiscoCore-R2-konfiguraatiot

```
Core-R1#sh run
Current configuration : 1992 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Core-R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 25
```

```
!
ip cef
!
interface Loopback1
 ip address 80.0.0.1 255.255.128.0
!
interface Loopback2
 ip address 85.0.128.1 255.255.224.0
!
interface FastEthernet3/0
 no switchport
 ip address 210.10.1.13 255.255.255.252
!
interface FastEthernet3/3
 description Link to Juniper-R5, port Ge-1/0/2
 no switchport
 ip address 210.10.1.6 255.255.255.252
!
interface GigabitEthernet3/0
 no switchport
 ip address 210.10.1.9 255.255.255.252
!
interface Vlan1
 no ip address
!
router bgp 101
 no synchronization
 bgp log-neighbor-changes
 network 80.0.0.0 mask 255.255.128.0
 network 85.0.128.0 mask 255.255.224.0
 neighbor 210.10.1.5 remote-as 100
 neighbor 210.10.1.10 remote-as 106
 neighbor 210.10.1.14 remote-as 102
 no auto-summary
!
ip http server
no ip http secure-server
!
end
```

Liite 19. CiscoCore-R3-konfiguraatiot

```
core-r3#sh run
Current configuration : 1756 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname core-r3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 25
```

```
!
ip cef
!
interface FastEthernet3/1
 no switchport
 ip address 210.10.1.18 255.255.255.252
 no shutdown
!
interface GigabitEthernet3/0
 no switchport
 ip address 210.10.1.25 255.255.255.252
 no shutdown
!
interface Vlan1
 no ip address
!
router bgp 103
 no synchronization
 bgp log-neighbor-changes
 network 200.30.0.0 mask 255.255.224.0
 network 200.35.0.0 mask 255.255.248.0
 neighbor 210.10.1.1 remote-as 100
 neighbor 210.10.1.17 remote-as 102
 neighbor 210.10.1.26 remote-as 106
 no auto-summary
!
ip http server
no ip http secure-server
!
end
```

Liite 20. CiscoCore-R4-konfiguraatiot

```
core-r4# sh run
Current configuration : 1455 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname core-r4
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
no ip dhcp use vrf connected
!
interface Loopback1
 ip address 100.80.192.1 255.255.192.0
```

```
 no shutdown
!
interface FastEthernet0/1
 ip address 210.10.1.33 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet2/0
 ip address 210.10.1.29 255.255.255.252
 negotiation auto
 no shutdown
!
router bgp 104
 no synchronization
 bgp log-neighbor-changes
 network 100.80.192.0 mask 255.255.192.0
 neighbor 210.10.1.30 remote-as 105
 neighbor 210.10.1.34 remote-as 106
 no auto-summary
!
ip classless
!
no ip http server
no ip http secure-server
!
end
```

Liite 21. CiscoCore-R5-konfiguraatiot

```
core-r5#sh run
Current configuration : 1549 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname core-r5
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
no ip dhcp use vrf connected
!
interface Loopback1
 ip address 30.10.0.1 255.255.0.0
 no shutdown
!
interface Loopback2
```

```
 ip address 191.145.224.1 255.255.224.0
 no shutdown
!
interface FastEthernet0/1
 ip address 210.10.1.37 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!

interface GigabitEthernet2/0
 ip address 210.10.1.30 255.255.255.252
 negotiation auto
 no shutdown
!
router bgp 105
 no synchronization
 bgp log-neighbor-changes
 network 30.10.0.0 mask 255.255.0.0
 network 191.145.224.0 mask 255.255.224.0
 neighbor 210.10.1.29 remote-as 104
 neighbor 210.10.1.38 remote-as 106
 no auto-summary
!
ip classless
!
no ip http server
no ip http secure-server
!
end
```

Liite 22. CiscoCore-R6-konfiguraatiot

```
Core-r6#sh run
Current configuration : 1821 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Core-r6
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
!
interface Loopback1
 ip address 150.40.64.1 255.255.192.0
 no shutdown
!
interface Loopback2
 ip address 196.197.208.1 255.255.240.0
 no shutdown
```

```
!
interface GigabitEthernet0/1
 description Link to Core-r1
 ip address 210.10.1.10 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no shutdown
!
interface GigabitEthernet0/2
 description Link to Core-r2
 ip address 210.10.1.22 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no shutdown
!
interface GigabitEthernet0/3
 description Link to Core-r3
 ip address 210.10.1.26 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no shutdown
!
interface FastEthernet1/0
 description Link to Core-r4
 ip address 210.10.1.34 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet1/1
 description Link to Core-r5
 ip address 210.10.1.38 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!
router bgp 106
 no synchronization
 bgp log-neighbor-changes
 network 150.40.64.0 mask 255.255.192.0
 network 196.197.208.0 mask 255.255.240.0
 neighbor 210.10.1.9 remote-as 101
 neighbor 210.10.1.21 remote-as 102
 neighbor 210.10.1.25 remote-as 103
 neighbor 210.10.1.33 remote-as 104
 neighbor 210.10.1.37 remote-as 105
 no auto-summary
!
!
no ip http server
no ip http secure-server
!
end
```

Liite 23. WG1-SW1-konfiguraatiot

```
wg1-sw1#sh run
Current configuration : 1820 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
!
hostname wg1-sw1
!
ip subnet-zero
ip routing
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp mode transparent
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan 10
 name VLAN10
!
vlan 20
 name VLAN20
!
vlan 130
 name Vlan130
!
vlan 1001
 name Vlan1001
!
interface GigabitEthernet0/3
 description Trunk to WG1-sw3, port 1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/7
 description PC in private IP address space
 switchport mode access
 switchport access vlan 10
!
interface Vlan10
 description Routing interface for VLAN10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 description Routing interface for VLAN20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan130
 description Public IP routing interface
 ip address 130.100.10.1 255.255.255.0
!
interface Vlan1001
 description Network between Operator
```

```
 ip address 130.100.8.2 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 130.100.8.1
end
```

Liite 24. WG1-SW3-konfiguraatiot

```
configure vlan Default delete ports all
disable ports all

create vlan vlan10
configure vlan vlan10 tag 10
configure vlan vlan10 add ports 1,5 tagged

create vlan vlan20
configure vlan vlan20 tag 20
configure vlan vlan20 add ports 1,5 tagged

create vlan vlan1001
configure vlan vlan1001 tag 1001
configure vlan vlan1001 add ports 1,5 tagged

enable ports 1,5
```

Liite 25. WG2-SW1-konfiguraatiot

```
wg2-sw1#sh run
Current configuration : 1820 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg2-sw1
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp mode transparent
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan 10
 name VLAN10
!
vlan 20
 name VLAN20
!
interface GigabitEthernet0/3
```

```
 description Trunk to WG2-sw3, port 1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/7
 switchport mode access
 switchport access vlan 10
!
ip classless
ip http server
!
end
```

Liite 26. WG2-SW3-konfiguraatiot

```
configure vlan Default delete ports all
disable ports all

create vlan vlan10
configure vlan vlan10 tag 10
configure vlan vlan10 add ports 1,5 tagged

create vlan vlan20
configure vlan vlan20 tag 20
configure vlan vlan20 add ports 1,5 tagged

enable ports 1,5
```